MAANPUOLUSTUSKORKEAKOULU

TAKTISEN (KOGNITIIVISEN) TIETOLIIKENNEJÄRJESTELMÄN KYBERTURVALLISUUDEN VAATIMUKSET JA TOTEUTUSVAIHTOEHDOT

Pro gradu -tutkielma

Yliluutnantti
Juuso Oinasmaa

Sotatieteiden maisterikurssi 9
Maasotalinja

Huhtikuu 2020

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Sotatieteiden maisterikurssi 9	**Maasotalinja**
Tekijä **Yliluutnantti Juuso Oinasmaa**	
Tutkielman nimi **TAKTISEN (KOGNITIIVISEN) TIETOLIIKENNEJÄRJESTELMÄN KYBERTURVALLISUUDEN VAATIMUKSET JA TOTEUTUSVAIHTOEHDOT**	
Oppiaine johon työ liittyy Sotatekniikka	Säilytyspaikka Maanpuolustuskorkeakoulun kirjasto
Aika Huhtikuu 2020	Tekstisivuja 97 Liitesivuja 40

TIIVISTELMÄ

Perinteisillä tietoliikennejärjestelmillä on monia haasteita spektrinhyödyntämisen, monimutkaisuuden, mukautettavuuden ja liikkuvuuden suhteen. Tämä on johtanut myös järjestelmien monimutkaisuuteen ja vaikeaan hallittavuuteen. Kognitiivisesta radiosta ja -tietoliikennejärjestelmistä pyritään löytämään tulevaisuuden ratkaisuja sähkömagneettisen spektrin ja verkonhallinnan optimointiin liittyvien tavoitteiden saavuttamiseksi.

Uusiin teknologioihin liittyy myös uudenlaisia uhkia. Tämän tutkimuksen tavoitteena on tutkia kognitiivisten tietoliikenneverkkojen yleisiä teknisiä ominaisuuksia ja kartoittaa kognitiivisen teknologian mukanaan tuomia mahdollisuuksia ja haavoittuvuuksia erilaisille kyberuhkille sotilaallisessa kontekstissa. Tunnistettujen haavoittuvuuksien suhteen tutkimuksen tavoitteena on löytää toteutusvaihtoehtoja järjestelmän kyberturvallisuuden parantamiseksi, ja asettaa vaatimuksia järjestelmän turvallisuuden kehittämiseksi.

Tutkimuksen teoreettinen viitekehys rakentuu erityisesti NATO:n kognitiivisia tietoliikennejärjestelmiä käsittelevän tutkimusraportin pohjalta. Tutkimusmenetelmänä käytetään triangulaatiota, joka ilmenee aineisto- ja menetelmätriangulaationa. Aineisto koostuu kirjallisuusaineistosta, jota on täydennetty asiantuntijakyselyillä delfoi-menetelmää käyttäen. Menetelmäriangulaatio näkyy kvantitatiivisen ja kvalitatiivisen tutkimusotteen hyödyntämisessä analyysivaiheessa. Delfoi-kyselyn tulokset kuvaavat asiantuntijoiden mielipiteitä järjestelmän tärkeimmistä ominaisuuksista, merkittävimmistä uhkista sekä kyberturvallisuuden toteutusvaihtoehdoista ja vaatimuksista.

Johtopäätöksenä kognitiivisen tietoliikennejärjestelmän päästä-päähän -tavoitteen toteuttamiseksi ja optimoimiseksi tarvitaan ohjelmistopohjaisia elementtejä kaikissa kerroksissa. Kognitiivinen radio ja -tietoliikennejärjestelmät tulevat muuttamaan elektronisen sodankäynnin luonnetta. Merkittävimmät haavoittuvuudet liittyvät järjestelmän protokollien ja taajuuspäätösprosessin manipuloitavuuteen yhdistetyllä kyber/ELSO-vaikuttamisella, kontrolliliikenteeseen sekä ohjelmisto-ohjatun tietoverkkoarkkitehtuurin keskitettyyn ohjaukseen. Kyberturvallisuutta parantaisi erityisesti SDN:n hajautettu arkkitehtuuri, verkon klusterointi ja hajaspektritekniikalla toteutetut dynaamiset kontrollikanavat.

AVAINSANAT

Kognitiivinen radio, kognitiivinen tietoliikennejärjestelmä, ohjelmisto-ohjattu tietoverkkoarkkitehtuuri, SDN, kyberuhkat, kyberturvallisuus, menetelmätriangulaatio, delfoi

TAKTISEN (KOGNITIIVISEN) TIETOLIIKENNEJÄRJESTELMÄN KYBERTURVALLISUUDEN VAATIMUKSET JA TOTEUTUSVAIHTOEHDOT

Sisältö

TAKTISEN (KOGNITIIVISEN) TIETOLIIKENNEJÄRJESTELMÄN KYBERTURVALLISUUDEN VAATIMUKSET JA TOTEUTUSVAIHTOEHDOT

1. JOHDANTO

1.1. Tutkimuksen tausta

Yksi tärkeimmistä menestyksen tekijöistä nykypäivän sotilasoperaatioissa on tietoylivoima. Kerätyn tiedon on oltava saatavilla oikeassa paikassa oikeaan aikaan kaikissa tilanteissa. Sen jakeluun käytetään tietoliikennejärjestelmiä. Nykyaikaisten tietoliikennejärjestelmien mukautuvuus kaikkiin mahdollisiin tilanteisiin on johtanut myös järjestelmien monimutkaisuuteen ja vaikeaan hallittavuuteen. Monimutkaisuudesta huolimatta optimitilanteessa tietoliikennejärjestelmät olisivat kestäviä, luotettavia, tehokkaita ja helppoja mukauttaa. [1, ES-1]

Verkostopuolustuksen doktriini asettaa runsaasti vaatimuksia tietoliikennejärjestelmälle verkostoituneessa taistelutilassa. Taktisen tietoliikenneverkon on mahdollistettava pääsy tietoon sekä tiedon turvallinen, tehokas ja jatkuva jakaminen eri toimijoiden välillä. Tietoliikenneteknologia on kehittynyt valtavasti viimeisten vuosikymmenten aikana, mikä on johtanut myös Puolustusvoimien tietoliikennejärjestelmien modernisointiin. Perinteisillä tietoliikennejärjestelmillä on kuitenkin monia haasteita monimutkaisuuden, mukautettavuuden ja käyttäjän tai solmun liikkuvuuden suhteen [2, s.19]. Puolustusvoimissa suurimpana viimeaikaisena taktisen tason tietoliikennejärjestelmien suorituskykyjä parantavana hankkeena on ollut maavoimien uusi tietoliikennejärjestelmä M18.

Yksi merkittävä muutos sotilastietoliikenteessä on ollut kaupallisten teknologioiden kehityksen seuraaminen ja kaupallisten ratkaisujen hyödyntäminen sotilaallisiin järjestelmiin. Kehittämisen seurauksena sotilaalliset tietoliikennejärjestelmät ovat myös monimutkaistuneet, mikä asettaa omat haasteensa niiden käytön ja hallinnan suhteen. Tästä johtuen tietoliikennejärjestelmien resurssien käyttö on vain harvoin optimaalista, ja edellä mainittujen monimutkaisten tietoliikennejärjestelmien ongelmia yritetään ratkaista kognitiivisten tietoliikennejärjestelmien tutkimuksella. [3, s. 2] Perinteisissä verkoissa verkon toimintaa sanelevat käytännöt on toteutettu enimmäkseen alemman tason laitekokoonpanoilla. Suurin osa tietoliikennejärjestelmien laitteista käyttää monimutkaisia ohjausprotokollia, joissa on suuri joukko konfiguroitavia parametreja. Valtava määrä verkotettuja laitteita ja suurten verkkojen ohjausparametrien konfiguroiminen hankaloittavat verkon toimintaa. Lisäksi nämä kokoonpanot ovat useimmiten alttiita inhimillisille virheille. [2, s. 19]

Kognitiivisesta radiosta ja -radioverkosta pyritään löytämään ratkaisuja radioverkoille käytön optimointiin liittyvien tavoitteiden saavuttamiseksi. Nämä ratkaisut perustuvat ajatukseen, että tulevat radioverkot pystyvät seuraamaan niiden sisäistä tilaa ja ulkoisia vaikutteita, kuten spektrissä tapahtuvia muutoksia, ja reagoimaan niihin itsenäisesti. Prosessia, jossa tarkkaillaan, tehdään päätöksiä havaintojen perusteella ja opitaan näistä päätöksistä, nimitetään kognitioksi. Siksi verkkoja, joilta löytyy nämä ominaisuudet, kutsutaan kognitiivisiksi radioverkoiksi. [1, ES s. 1] Uusien verkkoteknologioiden turvallisuudessa on kuitenkin usein vielä parantamisen varaa. Erityisesti tietoturva on ratkaisevassa osassa uusien verkkoteknologioiden menestymisessä.

Tämän tutkimuksen tarkoituksena on tutkia kognitiivisia (älykkäitä, automaattisia) toimintoja sisältäviä taktisia tietoliikennejärjestelmiä, jotka toteutuvat pääosin radioteitse. Työn tavoitteena on käsitellä kognitiivisten tietoliikennejärjestelmien yleisiä teknisiä ominaisuuksia ja kognitiivisen tekniikan mukanaan tuomia mahdollisuuksia ja haavoittuvuuksia. Ennusteiden mukaan kognitiivisilla ominaisuuksilla on sotatekniikassa tulevaisuudessa merkittävä rooli. Kognitiiviteknologia, sensoriteknologia ja verkostoitumisteknologia ovat kolme ensimmäistä yleisesti nimettyä teknologiaa, joilla voi olla disruptiivisia vaikutuksia sodankuvaan tai tapaan, jolla sotia tulevaisuudessa käydään [4, s. 19–22].

Ohjelmisto-ohjattujen radioverkkojen tutkimus on ajankohtaista M18-järjestelmän operatiivisen käyttöönoton myötä. Uusi kenttäviestijärjestelmä on jatkuvassa kehityksessä, ja ohjelmisto- ja laitevalmistajat tekevät päivityksiä järjestelmään sitä mukaa, kun uusia haavoittuvuuksia ja kehitystarpeita ilmaantuu. Järjestelmän ohjelmistopohjaisuus mahdollistaa järjestelmän jatkuvan kehittämisen sekä sen myötä myös kognitiivisten ominaisuuksien asteittaisen käyttöönoton. Lisäksi tutkimusaihe sivuaa useaa muuta tietoliikennejärjestelmiin liittyvää Puolustusvoimien aktiivista kehittämisohjelmaa.

Viime aikojen lukuisat uutisoinnit valtiollisten tahojen kohdistamasta kybervaikuttamisesta osoittavat, että halua ja kykyä käyttää kyberhyökkäyksiä on olemassa. Kyberuhkia käsittelevässä kappaleessa tarkastellaan erilaisia mahdollisia hyökkäys- ja vaikutustapoja (hyökkäysvektoreita), ja niiden kautta kartoitetaan kognitiivisen tietoliikennejärjestelmän turvallisuutta parantavia toteutusvaihtoehtoja ja vaatimuksia. Järjestelmän kognitiivisuus luo uusia mahdollisia vaikutusmekanismeja niin kyberhyökkäyksille kuin myös niin kutsutulle kyberelektroniselle sodankäynnille (engl. *Cyber/Electric Warfare*), jossa älykkäällä elektronisella vaikuttamisella voidaan vaikuttaa järjestelmään perinteisen tehokilpailun sijaan.

1.2. Tutkimustehtävä

Tutkimuksen pääkysymys on ”Mitä vaatimuksia ja toteutusvaihtoehtoja taktisen, kognitiivisen, tietoliikennejärjestelmän kyberturvallisuudelle tulisi asettaa?” Tutkimuksen pääkysymystä tarkastellaan uhkalähtöisesti, eli kartoittamalla kognitiiviseen tietoliikennejärjestelmään kohdistuvien uhkien vaikutusmekanismeja pyritään löytämään ratkaisuja järjestelmän kyberturvallisuuden parantamiseksi.

Tutkimuksen alakysymykset ovat:

- Mitä ominaisuuksia kognitiivinen tietoliikennejärjestelmä sisältää?
- Millaisia kyberuhkia on mahdollista kohdistua kognitiiviseen tietoliikennejärjestelmään?
- Miten nämä uhkat voisivat vaikuttaa järjestelmään?
- Miten kohdejärjestelmä voidaan suojata näiltä kyberuhkilta, ja miten kohdejärjestelmän kyberturvallisuutta voidaan parantaa?

Kirjallisuusselvityksen pohjalta järjestelmän teknisiä ominaisuuksia ja niiden tuomia sotilaallisia mahdollisuuksia käsitellään ensimmäisessä kappaleessa. Kirjallisuudessa esiin tulleita uhkia ja turvallisuutta parantavia toteutusvaihtoehtoja käsitellään kappaleessa 3. Kappaleen 4 sisältämä tutkimuksen delfoi-kyselyn ensimmäinen kierros on laadittu keräämään kotimaisten asiantuntijoiden (Puolustusvoimat, tiedeyhteisö ja teknologiateollisuus) näkemyksiä tutkimuksen pää- ja alakysymyksiin liittyen. Kyselyn tuloksia on analysoitu vertaamalla niitä kirjallisuusselvityksessä esiintyneisiin teemoihin. Kyselyn ensimmäisen kierroksen sekä kirjallisuusselvityksen pohjalta on laadittu toinen kyselykierros, jonka tulosten tarkoituksena on muodostaa näkemys asiantuntijoiden tärkeimpinä pitämiin asioihin tutkimuskysymyksiin liittyen. Johtopäätöskappaleessa on tehty yhteenveto kirjallisuuden ja delfoi-kyselyn perusteella. Tutkimusaihe on laaja ja hyvin tuore, mistä syystä tutkimuksen luonne on kartoittava.

1.3. Tutkimusmenetelmät ja rajaukset

Tutkimusmenetelmänä käytetään triangulaatiota, joka ilmenee erilaisten aineistojen (aineistotriangulaatio) ja tutkimusmenetelmien (menetelmätriangulaatio) käyttönä samassa tutkimuksessa. Aineistotriangulaatiossa yhdistetään useamman, tässä tapauksessa kahden aineiston (kirjallisuus ja kyselytutkimus) tulokset analyysin kautta yhdeksi tulokseksi. Menetelmätriangulaatio näkyy aineiston analysoinnissa kvalitatiivisin ja kvantitatiivisin menetelmin. Useimmiten menetelmätriangulaation käyttöä perustellaan sillä, että yksittäisellä tutkimusmenetelmällä ei tavoiteta riittävän kattavaa kuvaa tutkittavasta kohteesta. [5, s. 218] Aihealueen kirjallisuus ja tutkimustoiminta ovat laajaa, mutta aihealue on jatkuvassa muutoksessa. Tästä syystä myös tieto vanhenee nopeasti, ja viimeisimmän tietämyksen tavoittaminen on haastavaa.

Kirjallisuusselvityksen aineiston perusteella on ensin selvitetty, mitä viimeaikaisin tieto vastaa asetettuihin tutkimuskysymyksiin. Sen jälkeen delfoi-menetelmää käyttäen kyselyn ensimmäisen kierroksen avoimilla kysymyksillä kartoitettiin asiantuntijoiden esille nostamia teemoja tutkimuskysymyksiin liittyen. Avointen vastausten analysoinnissa on käytetty sekä laadullisen että määrällisen tutkimuksen piirteitä omaavaa sisällön erittelyä [6, s. 106–108]. Analyysissä keskityttiin yhteneväisyyksiin, eroavaisuuksiin sekä uusiin teemoihin, joihin kirjallisuusselvitys ei ottanut kantaa. Tämän analyysin pohjalta laadittiin delfoi-menetelmän kyselyn toinen kierros, jossa strukturoiduilla väittämillä kartoitettiin asiantuntijoiden konsensusta eri teemojen kohdalla. Väittämien vastausten kvantitatiivisella analyysilla saatiin tukea väittämien paikkansa pitävyydelle ja keskinäisille tärkeyssuhteille, sekä tutkimuksen yleistä luotettavuutta parannettua.

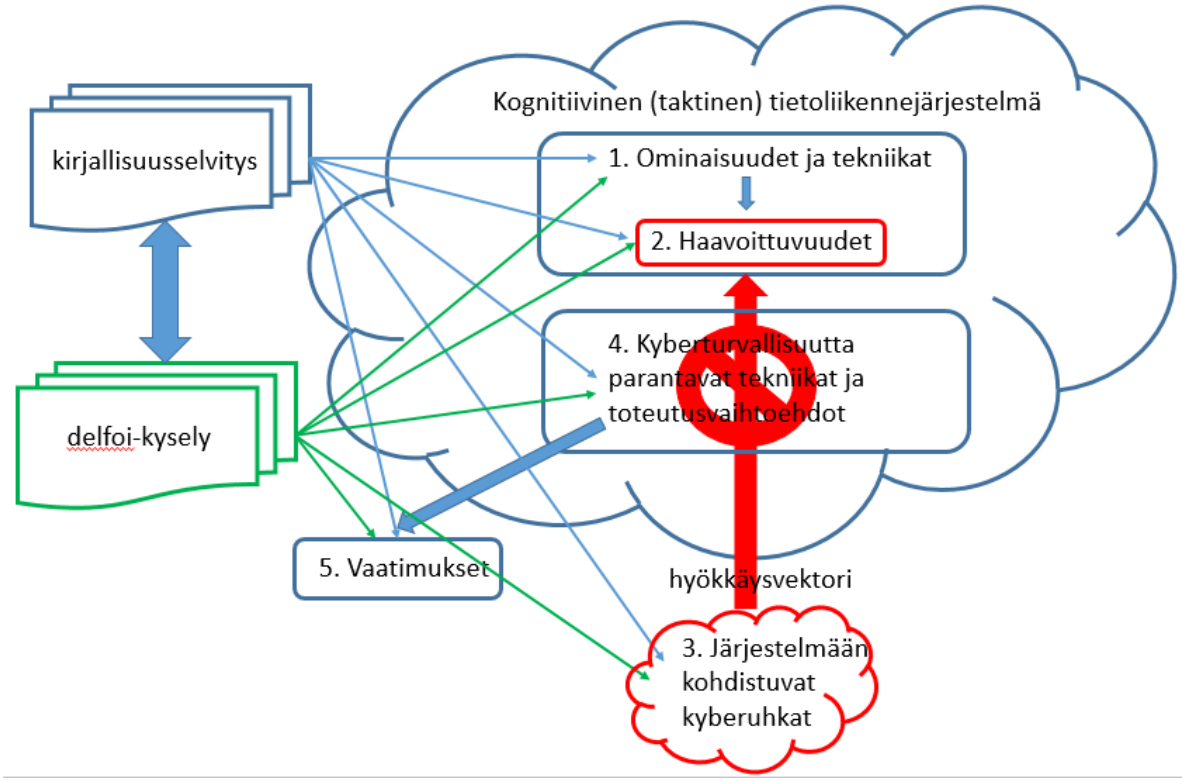
Tutkimuksen teoreettisen viitekehyksen tavoitteena on selvittää erityisesti kognitiivisten tietoliikennejärjestelmien tekniikkaa ja ominaisuuksia, sekä niihin kohdistuvia kyberuhkia induktiivisen päättelyn avulla. Teoreettisen viitekehyksen pohjana on käytetty erityisesti NATO:n tutkimusraporttia, jota on täydennetty muilla aihealueen tutkimuksilla, sekä eri tutkimustietokantojen avulla löydetyillä konferenssiesityksillä ja vertaisarvioiduilla tieteellisillä artikkeleilla. Tutkielman lähdemateriaalin koostamisessa on käytetty SCOPUS, Google Scholar ja IEEE-IET tietokantoja. Teoriaosuuden tavoitteena on kartoittaa viimeisin näkemys kognitiivisten tietoliikennejärjestelmien teknisistä ominaisuuksista ja selvittää niihin kohdistuvat kyberuhkat sekä turvallisuutta parantavat toteutusvaihtoehdot.

Tiedonhankintaa täydennetään kognitiivisten tietoliikennejärjestelmien sekä kyberuhkien asiantuntijoille kohdistetun kyselytutkimuksen avulla delfoi-menetelmällä, sekä analysoidaan saatuja tuloksia kvalitatiivisesti suhteessa kirjallisuusselvitykseen. Tutkimuksen analysoinnissa käytetään hyväksi myös kvantitatiivisia menetelmiä sovellettaessa asiantuntijakyselyn tuloksia delfoi-menetelmän avulla kahdessa iteraatiokierroksessa. Jyrkkä jako kvalitatiiviseen ja kvantitatiiviseen tutkimukseen on yksinkertaistava muun muassa tutkimusmenetelmien ja analyysitapojen moninaisuuden ja päällekkäisyyksien vuoksi [7]. Kun yksi tutkimusmenetelmä kuvaa kohdetta vain tietystä näkökulmasta, on useamman menetelmän käytöllä mahdollisuus parantaa tutkimuksen luotettavuutta [5, s. 193–204]. Kyselyn tutkimusjoukosta suurin osa on Puolustusvoimien palveluksessa olevia aihealueen asiantuntijoita. Lisäksi tutkimusjoukossa on tiedeyhteisön ja teknologiateollisuuden asiantuntijoita.

Kyselyt on toteutettu sähköpostiviestitse sekä Google Forms -kyselyalustaa käyttäen. Osaa asiantuntijoista haastateltiin kasvotusten kartoitettaessa tutkimuksen lähdeaineistoa ja perusjoukkoa. Kartoituksen pohjalta tutkimuksen varsinaisessa aineiston keruussa päädyttiin hyödyntämään kyselytutkimusta delfoi-menetelmällä. Kyselyn ensimmäinen kierros toteutettiin avoimin kysymyksin. Haastattelun sijaan kyselyyn päädyttiin aihealueen laajuudesta ja moniulotteisuudesta johtuen. Näin tutkittaville mahdollistettiin paremmin aikaa jäsennellä vastauksiaan ilman suoran vuorovaikutustilanteen luomaa painetta.

Verrattaessa kyselyä haastatteluun ne eivät ole toistensa synonyymejä, mutta niiden tiukkarajainen erottaminen ei ole silti aina mielekästä [6, s. 85]. Usein haastattelutilanteessa tutkija esittää suullisesti kysymyksiä tiedon antajalle, kun taas kyselyssä samanlaista vuorovaikutusta ei ole. Kuitenkin poikkeuksen muodostaa esimerkiksi sähköpostihaastattelu, jossa tutkija voi lähettää haastateltavalle tarkentavia kysymyksiä toisella kierroksella. Näin saadut vastaukset toimivat tutkimuksen aineistona [6, s. 85]. Tässä tutkimuksessa toinen kierros toteutettiin strukturoiduista väittämistä koostuvalla kyselyllä. Tutkimuksen asiantuntijajoukon vastausten pyrkimyksenä on kartoittaa pienehkön joukon mielipiteitä ja näkemyksiä, eikä tutkimuksella näin tavoitella laajaa yleistettävyyttä.

Tutkimuksen yleisluonne on menetelmältään kartoittava, eikä sitä ole rajattu vain tietynlaiseen kognitiiviseen tietoliikennejärjestelmään. Kognitiivisten tietoliikennejärjestelmien ominaisuuksien ymmärtämiseksi tekniikkaa on tarkasteltu yleisellä tasolla. Yleinen näkökulma tutkimuksessa on järjestelmätekninen. Taktiikkaa tarkastellaan vain siltä osin, kuin on tarpeellista teorian ja käsitteistön tulkitsemiseksi ja sotilaallisen viitekehyksen avaamiseksi. Taktiikan ja käyttöperiaatteiden tarkastelu ei kuitenkaan ole tutkimuksen tavoite. Kyberturvallisuuden ja kyberuhkien aihealue on todella laaja, ja niiden käsittely tässä tutkimuksessa on rajattu niihin kyberuhkiin, jotka ovat mahdollisia ensimmäisessä kappaleessa esitettyjä kognitiivisen tietoliikennejärjestelmän tekniikoita vastaan. Näihin kyberuhkiin on liitetty myös kyberelektroninen vaikuttaminen. Tutkimuksen viitekehys on esitelty kuvassa 1.



Kuva 1. Tutkimuksen viitekehys

1.4. Aiempi tutkimus ja lähdemateriaalin esittely

Tällä hetkellä erilaisten kyberaiheiden tutkimustilanne on hyvinkin laaja ja monipuolinen. Siitä syystä on mahdotonta käsitellä kaikkia keskeisiä tutkimuksia, joita kyberuhkiin ja kyberturvallisuuteen liittyen on toteutettu. Tutkimusaihe on sen verran tuore ja ajankohtainen, että kaksi tämän tutkielman tärkeintä primäärilähdettä on julkaistu tämän tutkimuksen aloittamisen jälkeen, vuosina 2018-2019. Tämän tutkimuksen primäärilähteinä on hyödynnetty erityisesti sotilaallisesta perspektiivistä tehtyjä tutkimuksia, jotka liittyvät tutkittavaan aihealueeseen. Tärkeimpänä tutkimuksen aihealueeseen liittyvänä kansainvälisenä tutkimuslähteenä on käytetty NATO:n tiede- ja teknologiaorganisaation heinäkuussa 2019 julkaisemaa laajaa kognitiivisia tietoliikennejärjestelmiä käsittelevää tutkimusraporttia ”COGNITIVE RADIO NETWORKS: EFFICIENT SOLUTIONS FOR ROUTING, TOPOLOGY CONTROL, DATA TRANSPORT, AND NETWORK MANAGEMENT”. Kotimaisista tutkimuksista tärkeimpänä primäärilähteenä on ollut vuonna 2018 Oulun yliopistolta valmistunut Ahmadin väitöskirja ”IMPROVING SOFTWARE DEFINED COGNITIVE AND SECURE NETWORKING”.

Maanpuolustuskorkeakoululla julkaistuja aihealuetta sivuavia tutkimuksia on Anssi Kärkkäisen vuonna 2013 julkaistu yleisesiupseerikurssin diplomityö ”A CYBER SECURITY ARCHITECTURE FOR MILITARY NETWORKS USING A COGNITIVE NETWORK APPROACH”. Kärkkäinen on tehnyt myös Aalto-yliopistolle vuonna 2015 edelliseen tutkimukseen perustuvan väitöskirjan ”DEVELOPING CYBER SECURITY ARCHITECTURE FOR MILITARY NETWORKS USING COGNITIVE NETWORKING”. Muita Maanpuolustuskorkeakoululla julkaistuja aihealuetta sivuavia tutkimuksia ovat Jussi Hongon vuonna 2015 tekemä yleisesiupseerikurssin diplomityö ”KOGNITIIVINEN RADIO SOTILAALLISEN MAANPUOLUSTUKSEN KONTEKSTISSA”, sekä Anssi Kärkkäisen vuonna 2011 tekemä esiupseerikurssin tutkielma "KOGNITIIVISET TIETOLIIKENNEVERKOT VERKOSTOPUOLUSTUKSESSA”. Lisäksi yleisesti taktisiin tietoliikennejärjestelmiin kohdistuvia kyberuhkia on käsitelty Ville Rantamäen vuonna 2018 valmistuneessa pro gradussa ”TAISTELUOSASTOON KOHDISTUVAT KYBERUHKAT”.

Kognitiivisista tietoliikenneverkoista ja niihin kohdistuvista kyberuhkista on löydettävissä hyvin vähän suomenkielisiä tutkimuksia tai artikkeleita. Aihe on hyvin globaali ja on ymmärrettävää, että tiedeyhteisössä saa laajempaa näkyvyyttä englanninkielellä tehdyillä tutkimuksilla. Tämä tutkimus onkin ensimmäisiä suomenkielellä julkaistuja aihealueen tutkimuksia. Yksi ohjelmisto-ohjattujen tietoliikennejärjestelmien tietoturvaa käsittelevistä suomenkielisistä lähteistä on Jyväskylän yliopistossa Siirosen vuonna 2018 julkaistu pro gradu -tutkielma ”PALVELUNESTOHYÖKKÄYKSEN VAIKUTUKSET OHJELMISTO-OHJATUN TIETOVERKON OHJAIMIIN”. Edellä mainittujen tärkeimpien lähdetutkimusten lisäksi pääosan lähdemateriaalista muodostavat eri tutkimustietokantojen avulla löydetyt konferenssiesitykset ja vertaisarvioidut tieteelliset artikkelit ja raportit, joiden koostamisessa on käytetty SCOPUS, Google Scholar ja IEEE-IET tietokantoja. Internetlähteistä on pyritty pääasiallisesti käyttämään lähteitä, jotka ovat joko yleisesti tunnettuja tietoturvaan tai tietotekniikkaan keskittyviä julkaisijoita tai usein viitattuja vertaisarvioituja artikkeleita, raportteja tai konferenssijulkaisuja sekä muissa tutkimuksissa viitattuja lähteitä.

Luotettavuuden analysointi tutkielmaa tehdessä on osin ollut haastavaa johtuen aihealueen luonteesta. Kognitiivisen tietoliikennejärjestelmän esitetyistä malleista tai konsepteista ei juurikaan ole olemassa käytännön sovellutuksia tai näyttöä, mistä syystä lähteen luotettavuuden osalta on tärkeää analysoida kirjoittajan tai lähteen kokonaiskompetenssia sekä jälleen viittausten määrää. Kyberuhkien suhteen voidaan arvioida jo toteutuneiden kybervaikutusten uhkaa kohdejärjestelmää kohtaan, mutta muodostuva uhka tulisi pyrkiä määrittelemään myös mahdollisten toteuttamattomien hyökkäysten varalle, koska vaikutusmekanismit ovat jatkuvan kehityksen alla. Kyberuhkien ennustaminen onkin erittäin hankalaa jopa aihealueen asiantuntijoille.

2. KOGNITIIVISET TIETOLIIKENNEJÄRJESTELMÄT

2.1. Kognitiivinen radio

Nykypäivänä langattoman tiedonsiirron osuus kasvaa edelleen räjähdysmäisesti. Tietyn tyyppiseen tiedonsiirtoon (tiedonsiirtonopeus vs. kantavuus) kelpaa vain tietyt taajuusalueet. Sähkömagneettisella spektrillä on kasvavissa määrin käyttäjiä, ja radiotaajuuskaistat alkavat olla luonnonvara, joka on Viestintäviraston taajuusjakotaulukonkin mukaan käytetty lähes loppuun. Kuitenkin todellisuudessa vain murto-osa varatuista taajuusalueista on aktiivisessa käytössä. Yksi syy kognitiivisen radion tarpeen kasvamiselle tulevaisuudessa onkin taajuusalueiden tehokkaampi käyttö. [8] Kognitiiviteknologian avulla pyritään löytämään ratkaisu kasvavista datansiirtovaatimuksista aiheutuvaan radiotaajuisen spektrin ahtauteen. [9] Voisi jopa sanoa, että kognitiivinen radio on vallankumouksellinen tekniikka, joka lupaa lieventää taajuuspulaa ja saavuttaa huomattavia parannuksia langattomaan tiedonsiirtoon. [10, s. 1]

Kognitiiviselle radiolle on useita erilaisia määritelmiä. Kognitiivisen radion perusajatus on, että järjestelmä kykenee itse oppimaan keräämistään tuloksista ja mukautumaan vallitsevaan tilanteeseen, ja siihen voidaan myös syöttää tietoa ulkopuolelta [11, s. 21]. Tämä älykäs toiminta perustuu niin kutsuttuun OODA-silmukkaan (*Observe-Orientate-Decide-Act*), jossa kognitiivinen radio jatkuvasti havainnoi ympäristöään, arvioi ja analysoi saatua tietoa sekä päättää ja toimii itsenäisesti ilman käyttäjän toimenpiteitä [12].

Vuonna 2008 Wireless Innovation Forum sopi ja hyväksyi muodollisesti kognitiivisen radion määritelmän, vaikkakin muutamalla huomautuksella. Tieteellisen kirjallisuuden, standardointielinten ja muiden asiaankuuluvien tahojen kognitiiviselle radiolle antamia termejä ja määritelmiä analysoitiin, ja Wireless Innovation Forum laati seuraavan määritelmän: “Kognitiivinen radio on lähestymistapa langattomaan tekniikkaan, jossa radio, radioverkko tai langaton järjestelmä on varustettu kyvyllä: [13]

- hankkia, luokitella ja järjestää tietoa (tietoinen, *aware*)
- säilyttää tietoa (tietoinen, *aware*)
- soveltaa logiikkaa ja analyysiä tietoihin (järki, *reason*)
- suorittaa valintoja radion, verkon tai langattoman järjestelmän toiminnallisista näkökohdista tarkoituksenmukaisen tavoitteen mukaisella tavalla (älykäs, *intelligent*)

NATO:n tutkimusraportissa [1] kognitiivinen radio määritellään seuraavasti: ”Kognitiivinen radio on älykäs langaton viestintäjärjestelmä, joka on tietoinen ympäröivästä ympäristöstään ja kykenee mukauttamaan asetuksiaan automaattisesti sähkömagneettisessa spektrissä tapahtuvien muutosten pohjalta. Ärsykkeet aiheuttavat vastaavia muutoksia tiettyihin toimintaparametreihin (esimerkiksi lähetysteho, kantoaaltotaajuus ja modulaatio) reaaliajassa, ottaen huomioon kaksi päätavoitetta: erittäin luotettavat yhteydet (ajallisesti ja alueellisesti) sekä radiospektrin tehokkaan hyödyntämisen.” [1, kpl 2, s. 2]

Määritelmän täyttäviä ominaisuuksia radioissa on ollut jo pitkään ohjelmistoradioissa, ja rajanveto kognitiivisen radion ja ohjelmistoradion välillä on häilyvä. Kognitiivinen radio, sekä pelkästään ohjelmistoradio kehittyneillä kognitiivisilla ominaisuuksilla, tuo huomattavia mahdollisuuksia parantaa langattoman tiedonsiirron toimintakykyä sotilaallisessa käyttöympäristössä. Suurimmat hyödyt sotilaallisessa kontekstissa liittyvät elektroniseen sodankäyntiin. Radioiden kognitiivisuuden myötä elektroniseen tiedusteluun voidaan varautua aiempaa tehokkaammin, ja elektronisen häirinnän osalta kognitiivisuus muuttaa toiminnan fundamentteja sekä mahdollistaa myös normaalin viestiaseman hyödyntämisen ELSO-asemana. [9] Tässä tutkimuksessa elektroninen sodankäynti ei ole kuitenkaan keskiössä, vaan sen sijaan koko tiedonsiirtojärjestelmän ohjelmistopohjaisuudesta aiheutuvan kyberuhkan merkittävyys arvioitaessa eri uhkien kokonaismerkityksiä.

Hongon [9] mukaan merkittävimmät suorituskyvyn parannukset sotilaallisessa kontekstissa saadaan seuraavista kognitiivisen radion ominaisuuksista: 1) dynaaminen spektrin hyväksikäyttö (DSA, *dynamic system access*) 2) yhteyksien adaptiivisuus ja radioresurssien hallinta (SLA, *single link adaptation* ja RRM, *radio resource management*) sekä 3) älykäs verkonmuodostus (SON, *self organized networks* ja RBR, *role based reconfiguration*). [9, s. 22-29]

Toiminnaltaan kognitiiviset radioverkot koostuvat ensisijaisista ja toisiokäyttäjistä. Ensisijaiset käyttäjät ovat taajuuskaistan ensisijaiset ”lisenssinhaltijat”. Toisiokäyttäjät käyttävät ensisijaisten käyttäjien taajuuksia silloin, kun ne eivät itse sitä tarvitse. Molemman tyypin käyttäjät käyttävät kognitiivisia kykyjään kommunikoida ja jakaa taajuuksia häiritsemättä toisiaan. [2, s. 32] Dynaaminen spektrinkäyttö DSA mahdollistaa toisiokäyttäjien (*secondary users*) ensisijaiselle käyttäjälle (*primary user*) allokoidun taajuusresurssin jakamisen. DSA:n myötä toisiokäyttäjien on teoriassa mahdollista jakaa taajuusresurssia aiheuttamatta häiriötä samalla taajuusalueella jo oleville järjestelmille. DSA:ssa radio suorittaa jatkuvaa spektrin analysointia, jonka jälkeen se erottelee signaalit kohinasta päättelemällä vastaanottamiensa spektrinäytteiden perusteella, ovatko signaalit päällä vai pois päältä. [9, s. 22-29]

Dynaaminen spektrinkäyttö on eniten tutkittu ajatus spektrin hyödyntämiseen. Tehokas taajuushavainnointi (SS - *spectrum sensing*) on avainroolissa DSA:ta käyttävän kognitiivisen radion toiminnan kannalta. Taajuuksien havainnointiprosessissa eri kanavalla tapahtuvilla vaikutuksilla (esimerkiksi häipyminen ja monitie-eteneminen) on erittäin tärkeä merkitys. Näiden taajuusominaisuuksien vaikutuksien vähentämiseksi on ehdotettu taajuuksien tunnistamisen jakelu- ja yhteistyömallia, toisin sanoen hajautettua taajuushavainnointia (DSS, *Distributed Spectrum Sensing*). Yhteistyömalli hyödyntää alueellista monimuotoisuutta toimintansa tehostamiseen. Yhteistyömallissa joukko kognitiivisia radioita muodostavat verkon, jossa lopullinen päätös taajuuden käytettävyydestä tehdään kaikkien kognitiivisten radioiden vastaanottaman tiedon perusteella. [14, s. 1] Jaettua taajuushavainnointia on käsitelty yksityiskohtaisemmin kappaleessa 2.3.4.

Yhteyksien adaptiivisuudella ja radioresurssien hallinnalla (RRM) tarkoitetaan prosessia, jossa radion eri parametreja, kuten teho, taajuus ja hypytysnopeus, hallitaan järjestelmätasolla ohjelmistollisesti. Se mahdollistaa resurssien optimoinnin lähetystehon, kanavien, tiedonsiirtonopeuden, modulaation ja aaltomuodon, koodauksen ja virheenkorjauksen hallinnoimisella. Kognitiivisesta radiosta puhuttaessa näiden ominaisuuksien optimointi tapahtuu automaattisesti. [9, s. 22-29]

Itsenäisesti organisoituvalla verkolla (SON) tarkoitetaan verkkoa, joka voi automaattisesti laajentua, muuntua ja konfiguroitua sekä optimoida verkon peittoaluetta, kapasiteettia, topologiaa, taajuusallokointia ja kaistanleveyksiä. Optimointikyky perustuu verkon kykyyn reagoida häiriöihin (kuten ELSO), signaalin vahvuuteen, paikkaan, viestiliikenteen toimintamalliin sekä muihin ympäristöllisiin ominaisuuksiin. [9, s. 22-29]

Tehtävän mukaisella konfiguroinnilla (RBR) tarkoitetaan sitä, että laite tai laitteet voidaan konfiguroida tarvitun tehtävän mukaan. Tällöin esimerkiksi komentajalla on radiossaan eri asetukset kuin ryhmänjohtajalla. Komentajalle annetaan mahdollisuus seurata useaa verkkoa yhtä aikaa, kun taas ryhmänjohtajalle riittää oman ryhmän verkko sekä joukkueenjohtajan verkko. Tämä ominaisuus parantaa erityisesti operaatioturvallisuutta. [9, s. 22-29]

2.2. SDN - ohjelmisto-ohjattu tietoverkkoarkkitehtuuri

Perinteiset tietoverkot ovat luonteeltaan dynaamisia ja monimutkaisia ja siten myös vaikeasti hallinnoitavissa ja muokattavissa. Perinteiset tietoverkot tuovat vain vähän mahdollisuuksia mukauttaa verkkoa ja sen käytäntöjä automaattisesti esimerkiksi toimintaympäristön, verkon käyttömäärän muutoksen tai tunkeilijan havaitsemisen perusteella. Tämä johtuu siitä, että tietoverkon hallinta on hajautettu yksittäisiin verkkolaitteisiin, jotka pitää kaikki konfiguroida erikseen. Nykyiset verkkolaitteet vaikeuttavat verkonlaajuisten käytäntöjen konfigurointia ja uusien, mukautuvien ominaisuuksien kehittämistä. Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri (SDN, *Software Defined Networking*) on yksi ratkaisumalli edellä kuvattuihin ongelmiin. [15, s. 1] Tieteellisen kirjallisuuden perusteella ohjelmisto-ohjattujen verkkojen alalla tapahtuukin nopeaa kehitystä. Esimerkiksi IEEE Xplore-tietokannassa oli 483 SDN:n liittyvää artikkelia vuonna 2012, kun taas samalla kyselyllä vuonna 2016 löytyi 2130 artikkelia. [1, kpl 4 s. 47; 16, kpl 4.4]

Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri tarkoittaa tietoverkon hallitsemista ja ohjaamista ohjelmistolla. Kuten perinteinen tietoverkko, se koostuu muun muassa reitittimistä ja kytkimistä. Se eroaa perinteisestä tietoverkosta kuitenkin siten, että reititinarkkitehtuurin hallinta- ja tiedonvälityskerros on erotettu toisistaan. Verkkolaitteet vain välittävät liikennettä, varsinainen verkon älykkyys on keskitetty hallintatasolle. Tästä syystä tietoverkon toimintaa voidaan muuttaa reaaliaikaisesti. Arkkitehtuuri on jaettu kolmeen tasoon, joista alimpana on verkkoelementtitaso (*data plane*), jonka lisäksi on sekä hallintataso (*control plane*) että verkkosovellustaso (*application plane*). Ohjelmisto-ohjattujen tietoverkkojen perusajatuksena on erottaa ohjausliikenne hyötyliikenteestä erillisiksi hallinta- ja verkkoelementtitasoikseen, jolloin verkkoelementtitasolla olevia reitittimiä voidaan yksinkertaistaa kytkimiksi, joita verkkosovellustason ohjelmisto ohjaa. [1, kpl 4 s. 41-47; 2, s. 27; 15, s. 1-5; 16, kpl 4.4]

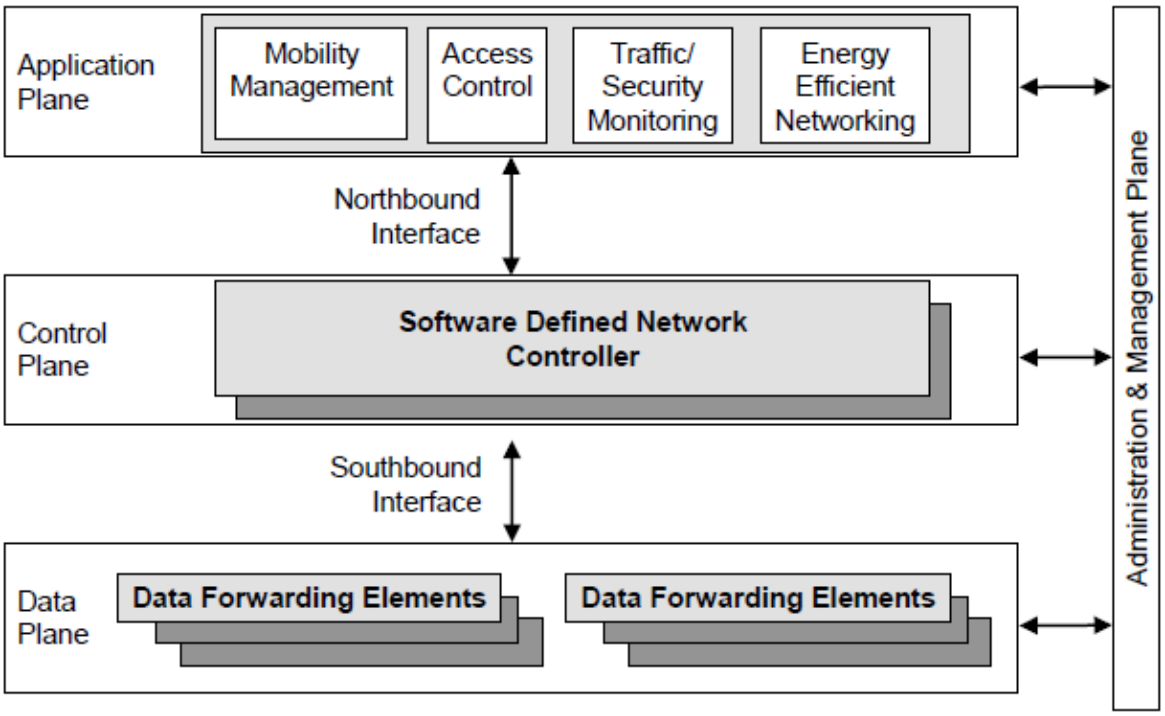
SDN-arkkitehtuurin olennainen osa on keskitetty ohjainohjelmisto, jolla voidaan hallita koko tietoverkkoa. Hallintataso on loogisesti keskitetty, ja on vuorovaikutuksessa verkkoelementtitasolla olevien kytkimien ja reitittimien kanssa ohjelmointirajapintojen (API, *application programming interface*) kautta. Verkkolaitteista on poistettu kaikki logiikka, jolloin ne sisältävät vain liikenteenvälitykseen vaadittavat toiminnot. Verkon älykkyys on siis keskitetty ylemmille hallinta- ja verkkosovellustasoille. Uusien ominaisuuksien toteuttaminen on helpompaa ohjelmallisesti kuin käyttäen verkkolaitteiden tarjoamia rajallisia toimintoja. Koska ohjaustaso on ohjelmoitu, eikä sitä ole asetettu kiinteään laiteohjelmistoon (*firmware*), uusia hallintatason toimintoja voidaan asettaa reaaliaikaisesti laitteisto- (*hardware*) tai laiteohjelmistosyklien sijaan. Lisäksi SDN-tietoverkkoa voidaan ohjata keskitetysti yhdestä paikasta, jolloin voidaan myös hyödyntää tietoja koko verkon tilasta. [1, kpl 4 s. 41-47; 2, s. 27; 15, s. 1-5; 16, kpl 4.4]

Ohjelmisto-ohjattu verkko perustuu siis kolmeen perusperiaatteeseen: fyysisen ja ohjelmistokerroksen erottamiseen, loogisesti keskitettyyn ohjaukseen ja verkkotoimintojen ohjelmoitavuuteen. Ohjelmisto-ohjauksen arkkitehtuuri muodostuu kahdesta pääkomponentista: hallintatasolla olevasta ohjaimesta (SDN Controller, SDN-C), jota voidaan kutsua myös verkkokäyttöjärjestelmäksi (NOS, *network operating system*), ja liikennetasolla olevasta liikennettä välittävästä laitteesta (SDN Forwarding Element, SDN-FE). Ohjain on loogisesti keskitetty toiminne ja verkossa on tyypillisesti yksi tai kaksi ohjainta. Niiden tehtävänä on määrittää kunkin liikennevuon reitit. Välityslaite, SDN-FE, muodostaa verkkoelementtikerroksen. Välitettävän datapaketin reitityksen määrittää ohjain ja reitityksen toteuttaa välityslaite. SDN-ohjain vastaa reittien valinnasta vastaanottajan osoitteen sijaan tietovuon perusteella. Ohjaimella voidaan toteuttaa joko keskitetty tai hajautettu liikenteenhallinta perustuen ohjaimen yhteyteen talletettuihin käytänteisiin. [1, kpl 4 s. 47-48; 15, s. 5; 16, kpl 4.4]

Vaikka perinteisten käyttöjärjestelmien avulla on hallittu alemman tason laitteita ja resursseja jo pitkään, tietoverkoissa tällainen lähestymistapa on kohtuullisen uusi. Ohjelmistopohjainen verkko keskittää loogisesti verkonhallinta-arkkitehtuurin, vapauttaa laitetason konfiguroinnin tarpeen, ei ole valmistajariippuvainen ja avaa tietoliikenneverkot monille innovaatioille [2, s. 20]. Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin ohjain toimii ikään kuin käyttöjärjestelmänä, joka piilottaa verkkolaitteiden erot ja tarjoaa ylemmälle kerrokselle laitteiden hallinnassa tarvittavat toiminnallisuudet. Ohjain kerää siis tietoja esimerkiksi verkon yleisestä tilasta, topologiasta, verkon laitteista ja konfiguraatiosta.

Hallinta- ja verkkoelementtitasojen välinen ohjelmointirajapinta perustuu avoimeen standardiin, jonka selvästi suosituin toteutus on OpenFlow-protokolla. [1, kpl 4 s. 47-48; 2, s. 28; 15, s. 5] OpenFlow-protokolla on yleisin standardoitu protokolla, jota käytetään ohjaimen ja kytkinten välillä. Kun tietovuo saapuu kytkimeen, kytkin välittää ensimmäisen paketin (paketit) ohjaimeen. Ohjain tekee päätökset pakettien reitittämisestä ja asentaa nämä päätökset kytkimeen käyttämällä OpenFlow-protokollaa. Päätökset ovat vuosääntöjen muodossa, jotka kuvaavat sen tietovuon sisältävien pakettien toiminnot. Vuosäännöt tallennetaan kytkimien vuotaulukoihin ja ohjain voi muuttaa näitä vuosääntöjä milloin tahansa. [2, s. 28]

Kuvassa 2 on esitetty NATO:n tutkimusryhmän näkemys SDN-arkkitehtuurista. Tällainen arkkitehtuuri tukee siis kolmea pääperiaatetta: ohjauslogiikan ja tiedonsiirron erottaminen, loogisesti (ei välttämättä fyysisesti) keskitetty ohjaus ja verkkotoimintojen ohjelmoitavuus. Nämä kolme pääperiaatetta tarkoittavat käytännössä sitä, että verkkotoimintojen hallinta, kuten datapakettien reititys tai edelleen lähettäminen, poistetaan reitittimiltä ja vaihdetaan yleisemmin saatavissa oleviin keskitettyihin ohjaimiin. Jokainen tällaisista ohjaimista voi ohjata paketin edelleen lähettämistä lukuisissa reitittimissä ja kytkimissä. [1, kpl 4 s. 47]



Kuva 2. SDN-arkkitehtuuri [1, kpl 4 s. 47]

SDN:n ohjaimet voidaan jakaa edelleen keskitettyihin ja hajautettuihin ohjaimiin. Keskitetty ohjain hallitsee kaikkia verkon laitteita yhdestä paikasta käsin, ja sen toimintavarmuus on siten kriittinen. Hajautetut ohjaimet voivat muodostaa keskitetyn klusterin tai fyysisesti hajautetun ryhmän. Hajautetut ohjaimet keskustelevat ohjainten välisen rajapinnan (*westbound API*) läpi. [15, s. 5-8] Loogisesti keskitettyä ohjausta on ehdotettu sisällyttämään lisäominaisuuksia, esimerkiksi ohjaustoiminnon jakamiseksi verkossa. Tämä on erityisesti asevoimien kannalta kiinnostava näkökulma, sillä keskitetty ohjaus voi muodostua kriittiseksi uhaksi (*Single-Point-of Failure*). Edellytys hajautetulle ohjaustoiminteelle on kuitenkin, ettei se omalla sisäisellä tietoliikenteellään aiheuta liikaa kuormaa. Hajautetun ohjauksen hyötyinä ovat sen robusti rakenne ja dynaaminen sopeutuvuus muuttuviin verkkotopologioihin. Se on samalla hyvä häiriösietoisuudeltaan, myös erilaisia kyberhyökkäyksiä vastaan. [1, kpl 4 s. 48; 16, kpl 4.4]

Hallintatason yläpuolella olevalla verkkosovellustasolla (*application plane*) toteutetaan tietoverkon logiikka, esimerkiksi reititys, kuormantasaus ja tietoturvapalvelut. Sovelluksia voidaan hyödyntää myös verkon virtualisoinnissa. Logiikan keskittämisen ansiosta ohjain voi hyödyntää koko verkon kattavia tietoja reitityksessä. Tämä edesauttaa ohjainta sopeuttamaan verkon käytäntöjä liikenteen muutoksiin nopeammin ja paremmin kuin mitä perinteisessä tietoverkossa on mahdollista. Ohjain voi hallita liikennettä hyvin yksityiskohtaisesti esimerkiksi yhden käyttäjän kokemuksen parantamiseksi. Ohjain voidaan myös toteuttaa hajautettuna järjestelmänä, jolloin skaalautuvuus paranee. Yksi vaihtoehto on hajauttaa ohjain väliaikaisesti useammalle fyysiselle laitteelle esimerkiksi siinä tapauksessa, että verkkoliikenteen ohjaus vaatii hetkellisesti tavallista enemmän resursseja. [15, s. 5-8]

SDN-tekniikan suurimpina hyötyinä nähdään sen helpottavan verkon suunnittelu-, käyttö- ja hallintaprosesseja [1, kpl 4 s. 41]. SDN helpottaa verkon reaaliaikaista käsittelyä ohjelmoitavien sovellusliittymien kautta ja varmistaa johdonmukaisen verkonlaajuisten käytänteiden toteuttamisen. Keskitettyä ohjainta käyttämällä SDN luopuu manuaalisten laitekonfiguraatioiden tarpeesta ja vähentää siten verkon monimutkaisuutta. [2, s. 20] SDN-arkkitehtuurin turvallisuudessa on kuitenkin parantamisen varaa. SDN-verkon ongelmia ovat muun muassa keskitetyn hallinnan turvallisuus, ohjaimen ja verkkolaitteiden viestinnän turvaaminen ja verkkosovellusten vahingollisen toiminnan estäminen. Tällä hetkellä turvallinen SDN-verkko tarkoittaa pysymistä yhden yrityksen tuotteissa, yhteyksien rajoittamista luotettujen laitteiden välille ja tiukkoja turvallisuuskäytäntöjä. Arkkitehtuurin täydet hyödyt jäävät tällöin saavuttamatta. Dynaaminen ja avoin SDN-tietoverkko voi kuitenkin olla perinteistä tietoverkkoakin turvallisempi, jos tunnistetut tietoturvaongelmat pystytään ratkaisemaan. [15, s. 2]

Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri on synnyttänyt myös ohjelmisto-ohjatun tietoturvallisuuden (SDSec, *Software-Defined Security*) käsitteen. Termillä tarkoitetaan turvallisuuteen liittyvien toimintojen loogista keskittämistä yhteen paikkaan sen sijaan, että ne sijaitsisivat erillisissä laitteissa ympäri verkkoa. SDSec-ohjain kykenee autentikoimaan verkkolaitteet ennen niiden yhdistämistä verkkoon. Tutkijoiden mukaan SDSec-ohjain voidaan erottaa tavallisesta SDN-ohjaimesta, jolloin se voisi hoitaa tietoturvallisuutta itsenäisesti. Yksi vaihtoehto on ohjelmisto-ohjattu tietoturva-arkkitehtuuri (SDSA, *Software-Defined Security Architecture*), joka erottaa turvallisuustoiminnot ja niiden hallinnan toisistaan. Sekä SDSec-ohjain että SDSA ovat esimerkkejä siitä, miten ohjelmisto-ohjatun tietoverkon tärkeintä ominaisuutta, hallinnan ja toimintojen erottamista, voidaan hyödyntää tietoturvan parantamisessa. [15, s. 16]

2.3. Kognitiivisen tietoliikennejärjestelmän määritelmä, arkkitehtuuri ja ominaisuudet

2.3.1 Määritelmä

Kognitiivisuudella tai kognitiolla tarkoitetaan ajatteluun, päättelyyn tai muistamiseen liittyviä tietoisesti älyllisiä toimintoja. Laajentamalla nämä ominaisuudet tietoliikennejärjestelmiin, kognitiivisilla tietoliikennejärjestelmillä on kyky havaita nykyiset verkko-olosuhteet, suunnitella, päättää ja toimia näiden havaintojen perusteella. Tärkein syy siihen, että tietoliikennejärjestelmille ehdotetaan kognitiivisia ominaisuuksia, on se, että tämänhetkiset tietoliikennejärjestelmät eivät sopeudu hyvin muuttuviin ympäristöihin. Muuttuva ympäristö saattaa johtua esimerkiksi muuttuvista verkko-olosuhteista, kuten ruuhkista joissakin solmuissa, palveluiden muutoksista, käyttäjien liikkeistä tai suojausasetusten ja käytänteiden muutoksista. [2, s. 31-32]

Kognitiivisten tietoliikennejärjestelmien tavoitteena on automatisoida tietoliikennejärjestelmät kyetäkseen reagoida ympäristön muutoksiin ilman mahdollista ihmisen puuttumista asiaan. Tietoliikennejärjestelmien kognition tarkoituksena on tarjota parempi päästä-päähän -suorituskyky; parantaa resurssien hallintaa, laadunvarmistusta ja tietoturvaa sekä täyttää muut verkon tavoitteet. Tehokas resurssienhallinta käyttäjän tarpeiden ja resurssien saatavuuden mukaan on ollut suuri haaste muun muassa verkko-operaattoreille. Langattomissa verkoissa tärkein ja riittämättömin resurssi on ollut taajuusspektri. Kognitiivinen radioverkko, joka käyttää kognitiota radiosolmuissa, tarjoaa ratkaisun haasteeseen mahdollistamalla taajuuksien jakamisen käyttäjien kesken reaaliaikaisesti. [2, s. 31-32]

Jotta radioverkko voi mukautua muuttuvaan ympäristöön, tulee kognitio tuoda mukaan koko verkkoon, ei vain päätelaitteeseen. Tämä eroaa olemassa olevista MANET-protokollista (*Mobile Ad Hoc Network*). Nämä verkkoprotokollat voivat mukauttaa vain verkkotopologiaansa, mutta eivät verkon käyttäytymistä olosuhteiden muuttuessa. Kognitiivinen tietoliikennejärjestelmä eroaa myös ohjelmisto-ohjatusta tietoliikenneverkosta, koska vaikka SDN voi säätää nopeasti verkon käyttäytymistä, siitä puuttuu kognitio ja tietoisuus ympäristöstä ja siten myöskin tieto siitä, mihin sopeutua. Kognitiivinen tietoliikennejärjestelmä eroaa myös kognitiivisesta radiosta (CR), koska kognitiivinen radio on tietoinen vain paikallisesta spektriympäristöstä ja siten tarkoitettu optimoimaan vain point-to-point -radiolinkit kykenemättä optimoimaan kokonaisuutta verkon suorituskyvyn suhteen. [1, kpl 1 s. 1]

Kognitiivinen radioverkko (CRN, *Cognitive Radio Network*) on verkko, joka voi tunnistaa ympäristönsä, säätää verkon käyttäytymistä vastaavasti ja oppia aiemmista kokemuksista. Tämä ei ole yksinkertainen tehtävä, mistä syystä tällaisia verkkoja ei ole vielä olemassa. Tekniikan odotetut hyödyt ovat kuitenkin merkittäviä. Radioverkko, joka pystyy optimoimaan verkon käyttäytymistä muuttuvissa olosuhteissa antaa parhaan mahdollisen suorituskyvyn ilman manuaalisia laitteiden uudelleenmäärityksiä. Tämä tarkoittaa verkonhallinnan suhteen sitä, että voidaan keskittyä itse tehtävän suorittamiseen joutumatta toteuttamaan vaikeita verkonmääritystehtäviä operaation aikana. Myös tekninen konfigurointi ennen operaatioita vähenee. [1, kpl 1 s. 1]

Kärkkäinen [3] määrittelee kognitiivisen tietoliikennejärjestelmän seuraavasti: ”Kognitiivinen tietoliikenneverkko on älykäs tietoliikennejärjestelmä, joka tiedostaa järjestelmän sisäisen sekä ympäristön tilan, tekee päätöksen verkon mukauttamisesta annetun tavoitteen saavuttamiseksi ja sen jälkeen konfiguroi verkon asetukset uudelleen. Keskeinen tekijä prosessissa on oppiminen eli kyky hyödyntää aiemmin tehtyjä päätöksiä.” Kognitiivisella tietoliikennejärjestelmällä on siis kolme perusominaisuutta: tilannetietoisuus, oppimis- ja päätöksentekokyky sekä täysin kontrolloitavat tietoliikenneparametrit ja -asetukset, joista voidaan johtaa kognitiiviset perustoiminnot: havainnointi, oppiminen, päätöksenteko, itseohjautuvuus ja automaattinen konfiguroituminen. [3]

Ahmad [2] määrittelee väitöskirjassaan kognitiivisen tietoliikennejärjestelmän vastaavasti: ”Kognitiivisilla verkoilla on kyky tarkkailla käyttäjän tarpeita, havaita käyttöympäristö ja sopeutua vastaavasti käyttäjän tarpeiden täyttämiseen kyseisessä ympäristössä. Kognitiivinen radioverkko (CRN, *Cognitive Radio Network*), joka toteuttaa kognitiivisen verkottumisen, pystyy tunnistamaan vapaat tai varatut radioresurssit ja mahdollistamaan siten resurssien yhteistyöhön perustuvan älykkään käytön. Täysin kognitiivinen verkko tarvitsee myös ylempien kerrosten olevan reaaliaikaisesti konfiguroitavissa, mistä syystä SAN-elementtejä (*Software Adaptable Network*) tarvitaan verkon reaaliaikaiseen konfiguroimiseen ohjelmiston avulla. Esimerkiksi taajuushallinta ja verkonmuodostus vaativat yhteistyötä kaikkien kerrosten välillä, mukaan lukien sovellus-, kuljetus-, verkko-, ja fyysiset kerrokset.” [2, s. 20]

NATO:n tutkimusraportissa [1] kognitiivisen tietoliikenneverkon määritelmässä on seuraavia ominaisuuksia: [1, kpl 2, s. 4]

- Solmuista (*node*) koostuva verkko, joka valitsee ja optimoi älykkäästi parametreja verkon päästä päähän -vaatimusten perusteella.

- Kognitiivisista radioista muodostuva verkko, jossa jokaisessa solmussa kerätty tieto jaetaan ja päätökset voidaan tehdä hajautetulla tavalla. Abstraktissa mielessä kognitiosta tulee sitten verkon, eikä yksittäisen radion toiminto.

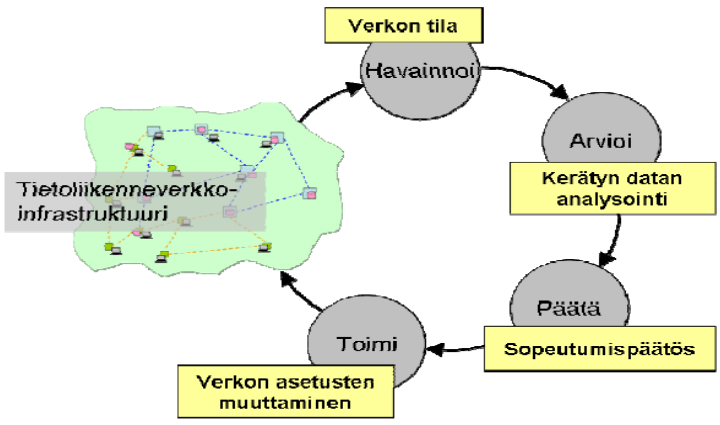
Kognitiivisen verkon yksittäisenä elementtinä käytetään yleisesti termiä solmu (*node)* ”radioyksikön” tai ”radiolaitteen” sijasta. Lopputulemana on määritelmä, jossa kognitiivinen radioverkko on verkosto, joka koostuu kognitiivisistä solmuista ja joka pystyy muodostamaan paikallista tietoa ympäristöstään (spektri ja verkko). Lisäksi verkko kokonaisuutena pystyy suorittamaan kognitiivisia toimintoja saavuttaakseen verkon yleisen tavoitteen (esimerkiksi tehokas päästä päähän -yhteys tai tehokas taajuuksien hyödyntäminen). [1, kpl 2, s. 4-5]

NATO:n tutkimusryhmä on luonut myös käsitteen kognitiivinen mobiili ad hoc -verkko (CRAHN, *Cognitive Radio Ad Hoc Network*), jolla on potentiaalia erityisesti sotilaallisissa käyttötarkoituksissa. CRAHN voidaan erottaa infrastruktuuriverkoista yleisen monihyppyarkkitehtuurin, dynaamisen verkkotopologian sekä ajan ja sijainnin mukaan vaihtelevan spektrin saatavuuden mukaan. [1, kpl 2, s. 5] CRAHN:ia on käsitelty tarkemmin kappaleessa 2.3.3.

2.3.2 Järjestelmän arkkitehtuuri, ominaisuudet ja toiminta

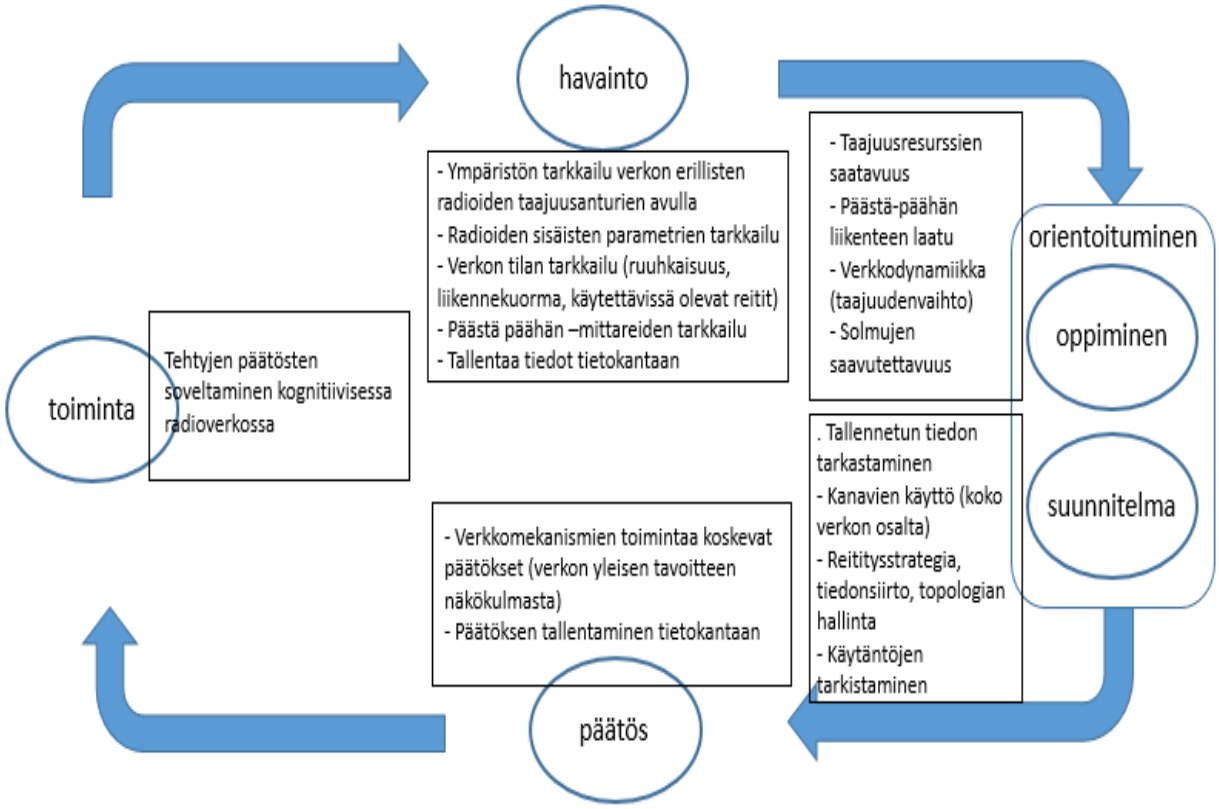
Kognitiivisen tietoliikenneverkon määritelmään kuuluu tavoitteellisuus, ns. ”päästä päähän” -malli (*end-to-end*). Tämä päästä-päähän -termi sisältää tässä yhteydessä kaikki ne verkon osat, jotka tarvitaan datavirran siirtämiseen. Päästä-päähän -ketju voi muodostua esimerkiksi aliverkoista, reitittimistä, kytkimistä, virtuaaliyhteyksistä, salausjärjestelmistä, siirtomedioista, rajapinnoista tai aaltomuodoista. Päästä-päähän -tavoite saa aikaan verkon laajuisen kognitiivisen luonteen, mikä edellyttää edellä mainittujen elementtien olevan ohjelmistopohjaisesti konfiguroitavissa. Ilman näitä tekijöitä järjestelmä voi sisältää kognitiivisia osia (esimerkiksi kognitiivinen radio), mutta järjestelmä ei ole kokonaisuudessaan kognitiivinen tietoliikennejärjestelmä. Edellä mainittu määritelmä tarkoittaa käytännössä sitä, että verkko voi itsenäisesti modifioida eri verkkokerroksia tietoliikenneverkon solmuissa. Esimerkiksi sähköisesti ohjatuilla antenneilla varustettu radio voi muodostaa kognitiivisen verkon, mikäli järjestelmä on tietoinen antennin ohjauksen vaikutuksesta koko verkon suhteen. Radioista ei sen sijaan muodostu kognitiivista verkkoa, mikäli radiojärjestelmä on tietoinen vain antennin konfiguroinnin muutoksen vaikutuksesta linkin laatuun, eikä tiedosta muutoksen vaikutusta muihin verkon solmuihin. [17]

Yleisen näkemyksen mukaan kognitiivisen tietoliikenneverkon oppiminen tapahtuu OODA-palautesilmukan mukaisesti (kuva 3) [3; 9]. Tässä prosessissa kognitiivinen järjestelmä tarkkailee ympäristöään ja verkon tilaa, minkä jälkeen järjestelmä arvio ja analysoi verkon ja ympäristön tilaa suhteessa haluttuun tavoitetilaan. Päätösvaiheessa tietoliikennejärjestelmä päättää, miten verkon asetuksia muutetaan. Lopuksi järjestelmä säätää verkon parametrit ja havainnoi muutoksen vaikutusta. Oppiminen on prosessissa kriittistä, sillä järjestelmän tulisi osata korjata päätöksentekoaan, mikäli muutoksen vaikutus on negatiivinen. [3, s. 20-21] Yksittäisen solmun ja verkon tavoitteiden välisten optimointiristiriitojen välttämiseksi järjestelmässä tulisikin olla konfliktien purkamisprosessi. [1, kpl 2 s. 5]



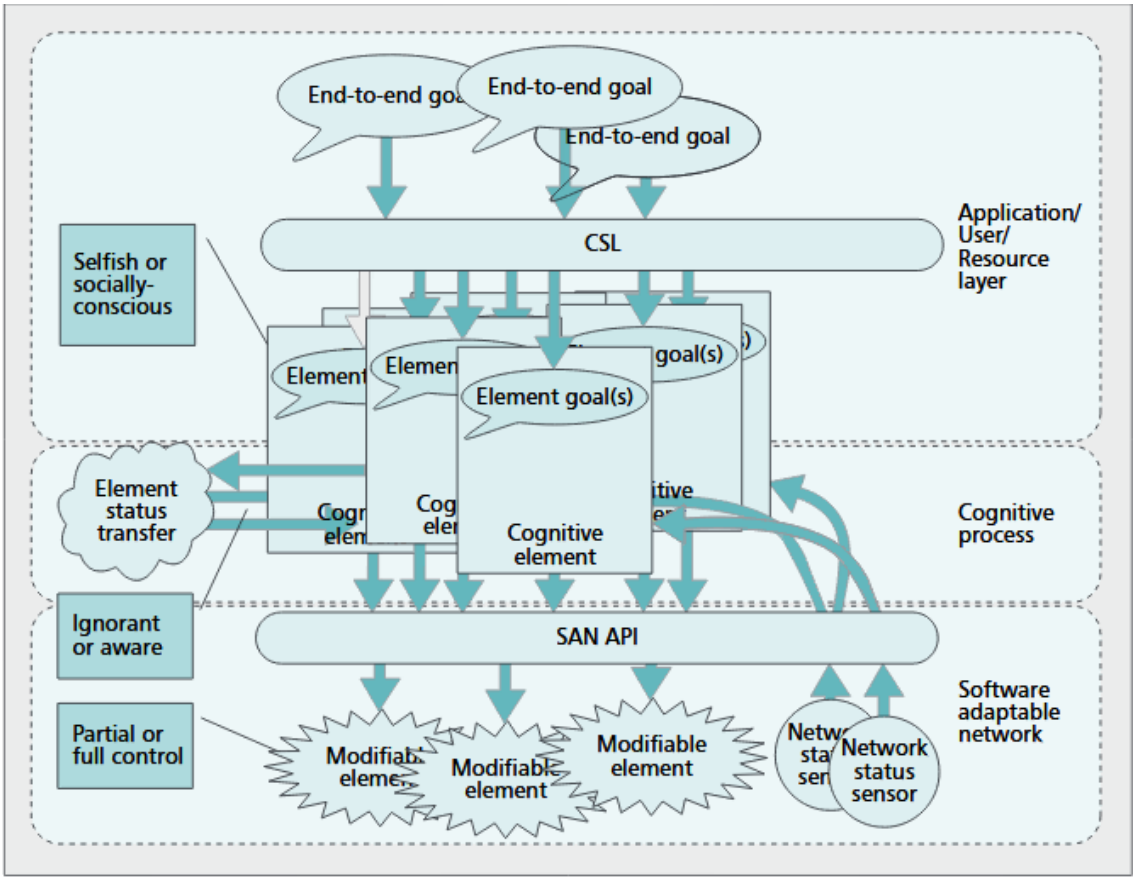
Kuva 3. Kognitiivisen tietoliikenneverkon palautesilmukka (OODA-silmukka) [3, s. 21]

Kun OODA-silmukkaan lisätään verkon toiminteet kussakin vaiheessa, voidaan järjestelmän toimintaa kuvata kognitiivisella syklillä. Verkon kognitiivinen sykli on havainnollistettu kuvassa 4. [1, kpl 2, s. 5]



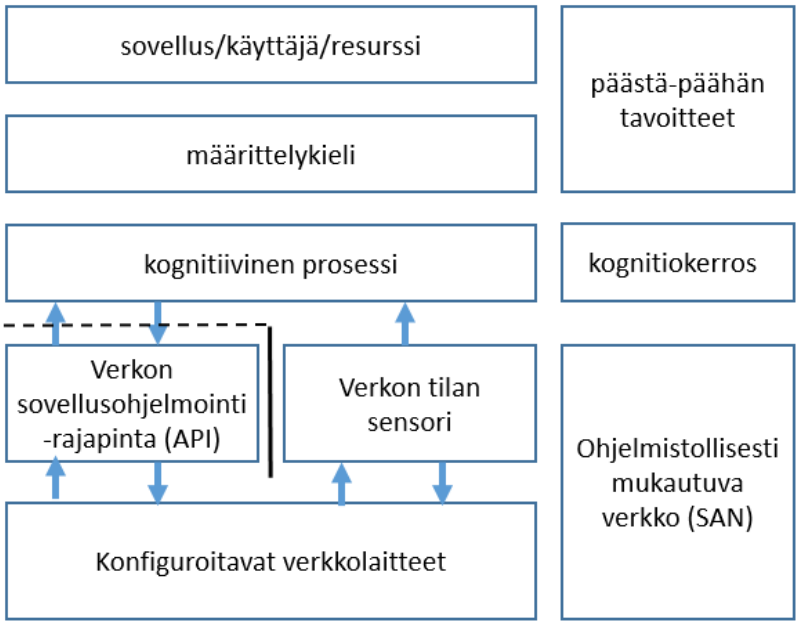
Kuva 4. Verkon kognitiivisen syklin toiminnallisuudet [1, kpl 2, s. 4]

Kuvassa 5 on esitetty kognitiivisen tietoliikennejärjestelmä kolmikerroksisena mallina. Tämän kolmikerroksisen mallin ylin kerros muodostuu järjestelmän ja verkkoelementtien tavoitteista (*end-to-end goal*), jotka määrittävät verkon käyttäytymistä. Nämä tavoitteet antavat syötteitä kognitiiviselle prosessille, joka määrittää järjestelmän suorittamat toimenpiteet. Mallin alimmalla kerroksella on ohjelmistolla muokattava verkko (SAN, *Software Adaptable Network*), joka sisältää järjestelmän fyysisen ohjauksen ja toimii kognitiivisen prosessin toimintaulottuvuutena. [17]



Kuva 5. Kognitiivisen tietoliikenneverkon kolmikerroksinen malli [17]

Ahmad [2] on yksinkertaistanut väitöskirjassaan kognitiivisen tietoliikenneverkon mallin kuvan 6 mukaisesti. Tässäkin mallissa kognitiivisella verkolla on kolme kerrosta. Päästä-päähän -päämäärät johtavat koko järjestelmän käyttäytymiseen, ja verkon käyttäjät, resurssit tai sovellukset määrittelevät ne. Kokonaispäämäärät välitetään kognitiiviselle prosessille kognitiokerroksessa määrittelykielen avulla. Kognitiivinen kerros koostuu kognitiivisesta prosessista, joka vastaa todellisesta päätöksenteosta päästä-päähän tavoitteiden ja nykyisen verkon tilan perusteella. Verkon päivitykset toimitetaan joko verkon sovellusliittymillä tai antureilla. Ohjelmistolla muokattava verkkokerros koostuu konfiguroitavista verkkoelementeistä, joita kognitiivinen prosessi voi konfiguroida reaaliaikaisesti. [2, s. 32]



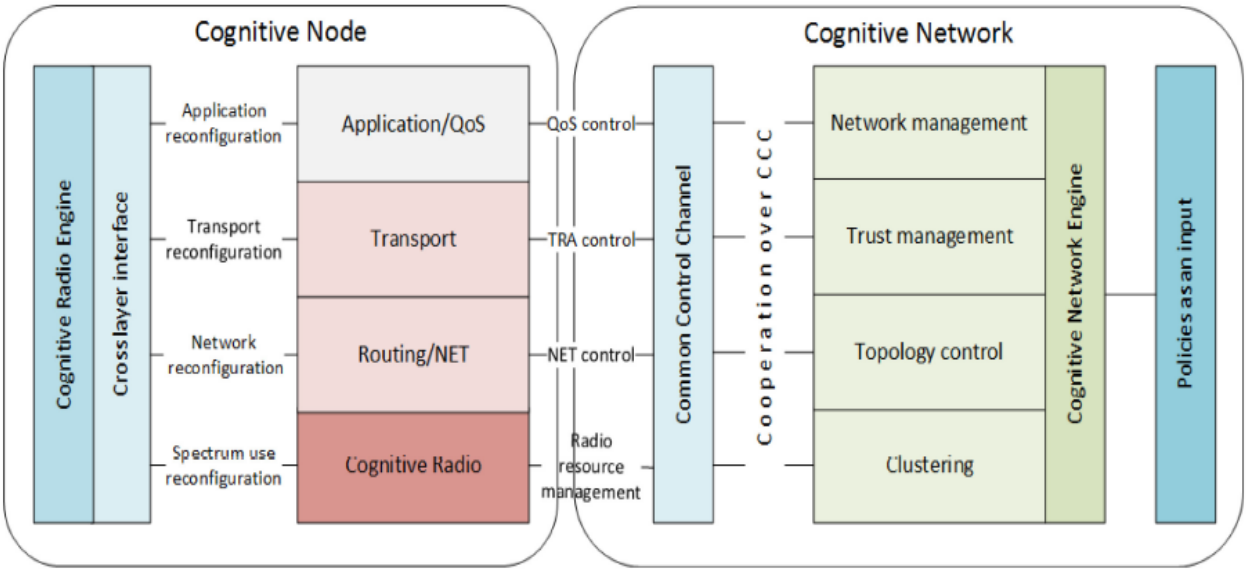
Kuva 6. Kognitiivisen tietoliikenneverkon malli [2, s. 32]

Jotta verkon käyttäjät kykenevät kytkemään tavoitteita kognitiiviseen prosessiin, tarvitaan käyttöliittymä. Tämä tapahtuu kognitiivisen määrittelykielen (CSL, *Cognitive Specification Language*) avulla. Tämä määrittelykieli ohjaa kognitiivisten elementtien toimintaa kääntämällä päästä-päähän -tavoitteet paikallisten, yksittäistä verkon osaa ohjaavien elementtien tavoitteiksi. Tämä kognitiivinen prosessi voidaan mieltää koneoppimiseksi, jolloin prosessissa voidaan hyödyntää erilaisia tekoälyyn, päätöksentekoon ja mukautuviin algoritmeihin liittyviä tekniikoita. [17] Täysin kontrolloitavat eli ohjattavat verkon elementit ovat edellytys kognitiivisen verkon maksimaaliselle suorituskyvylle, ja ideaalitilanteessa kaikki verkkoelementit ja parametrit ovat kognitiivisen kerroksen ohjattavissa. Kaikki verkon elementit eivät kuitenkaan välttämättä ole muokattavissa, mikä on huomioitava kognitiivisessa kerroksessa. [3, s. 26].

Kognitiivisen kerroksen toiminta perustuu syötteenä tulleen informaation määrään ja tietoisuuteen, jolloin verkon solmujen tulisi jakaa kaikki informaatio mahdollisimman tehokkaasti keskenään. Tämä asettaa keskeiseksi haasteeksi informaation tehokkaan jakamisen verkon solmujen välillä. Todellisuudessa päätöksenteon perustana oleva informaatio ei ole aina täydellistä ja päätöksenteossa on hyväksyttävä informaatiopuutteet [3, s. 25]. Informaatiopuute voi tarkoittaa, että solmut eivät tiedä tarkkaan muiden solmujen tavoitteita tai käytöstä. Informaation jakamisessa voidaan joutua optimoimaan kaista hyötylähetteen ja taustainformaation välillä. Solmujen väliselle jaetulle informaatiolle voidaan myös asettaa suodattimia, jotka estävät mahdollisesti irrelevantin informaation jakamisen kognitiivisille prosesseille keventäen näin järjestelmän kokonaiskuormitusta. [17]

Kognitiivisen tietoliikenneverkon alin kerros, ohjelmoitava verkko (SAN, *Software Adaptable Network*) muodostuu ohjelmointirajapinnasta (API), muokattavista verkkoelementeistä ja verkon tilaa mittaavista antureista, jotka tuottavat tarvittavan datan verkon tilasta. SAN ei varsinaisesti kuulu kognitiivisten verkkojen tutkimusalueeseen, mutta kognitiivisen prosessin tulee olla tietoinen sovelluskäyttöliittymästä ja rajapinnoista. Verkon tilasta voidaan tuottaa havaintoja paikallisesti (esimerkiksi kaistanleveys, bittivirhesuhde, akun kesto) tai laajemmin verkon suhteen (esimerkiksi viive, topologia). [17]

NATO:n tutkimusraportissa [1] on esitetty kuvan 7 mukainen arkkitehtuurimalli kognitiiviselle radioverkolle. Kuva mallintaa kognitiivisen solmun ja kognitiivisen radioverkon avaintoiminnot. Kuva erottaa solmun keskitetyt toiminnot (kognitiivinen solmu vasemmalla) verkonlaajuisista toiminnoista (kognitiivinen verkko oikealla). [1, kpl 4 s. 1]

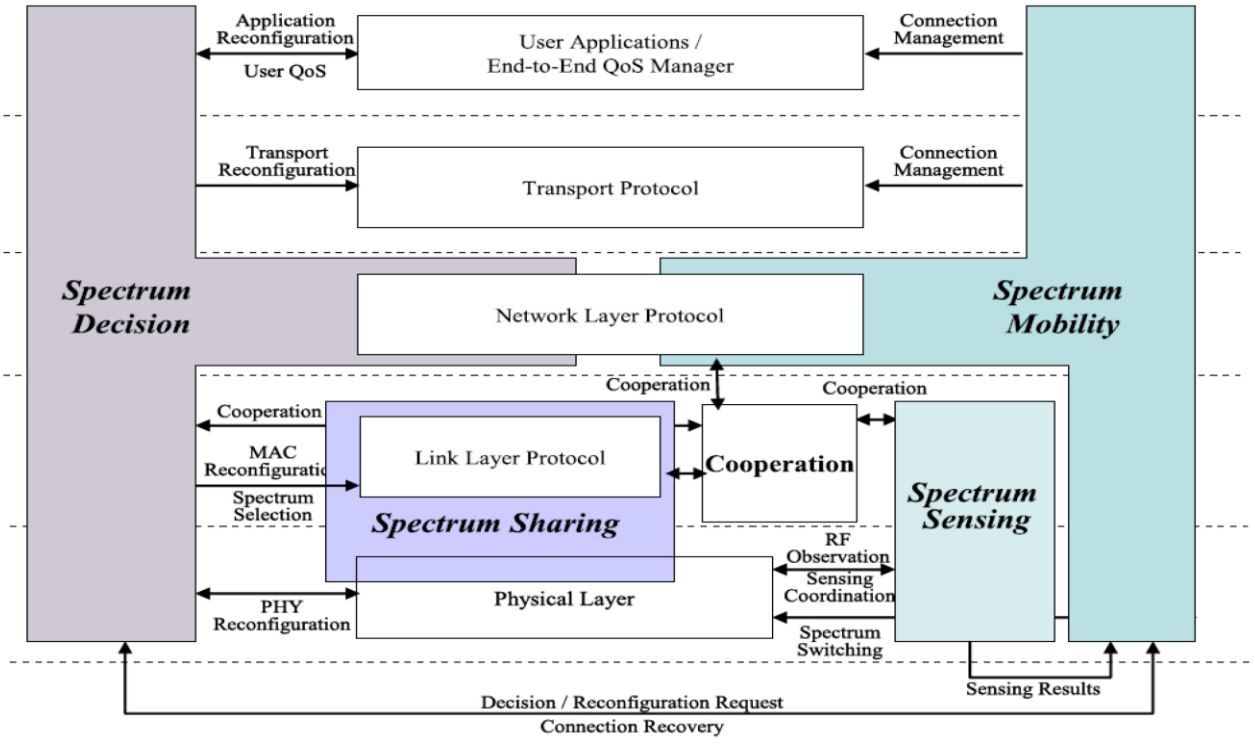


Kuva 7. Arkkitehtuurikuva kognitiivisen solmun toiminnan ja kognitiivisen verkon toimintojen välillä [1, kpl 4 s. 1]

Keskeinen tekijä solmukeskeisessä näkymässä on toiminnallisuudet eri kerrosten rajapintojen välillä sekä kognitiivisen moottorin (CRE, *Cognitive Radio Engine*) sisällyttäminen siihen. Tekniikka mahdollistaa radiosolmun kaikkien kerrosten jatkuvan uudelleenkonfiguroinnin kognitiivisen moottorin harkitsemien päätösten ja asetettujen käytänteiden ja strategioiden mukaisesti. Kognitiivinen radioverkko vaatii toisaalta tueksi yhteisen kontrollikanavan (CCC, *Common Control Channel*), joka toimii avainelementtinä koko verkon yhteisen ohjaamisen suhteen. Mainitut radiosolmukerrokset voivat käyttää yhteistä kontrollikanavaa myös suorittaakseen koko verkon laajuisia toimintatavan uudelleenmäärityksiä. Tämä tarkoittaa myös sitä, että kognitiiviset solmut osaavat hallita tai ainakin osallistuvat verkonlaajuiseen taajuuksien käyttöön ja koordinointiin. [1, kpl 4 s. 1]

Kognitiiviset solmut sekä tekniikat, jotka käyttävät yhteistä kontrollikanavaa verkonlaajuisiin konfiguraatioihin, mahdollistavat kognitiivisen verkottumisen. Kognitiivisen radioverkon toiminnan kannalta tärkeimmiksi arvioituja tekniikoita ovat klusterointi, topologian hallinta, luottamuksen hallinta ja yleinen verkonhallinta. Esimerkiksi kognitiivinen reititys ja topologian hallinta ovat tiiviisti toisiinsa nivoutuneita prosesseja verkkotasolla. Kuljetuskerros huolehtii päästä päähän -yhteyksien ja ruuhkien hallinnasta. Klusterointi on sen sijaan monimutkainen prosessi, jota voidaan soveltaa moniin tarkoituksiin kognitiivisen radioverkon toiminnassa. Verkonhallinnan tavoitteisiin sisältyy verkon yleinen luotettavuus, tehokkuus ja tiedonsiirtokapasiteetti. Verkonhallinta sisältää tavoitteet, strategiat ja käytännöt, joita ohjataan kognitiivisessa moottorissa. Kognitiivinen moottori viime kädessä sanelee, kuinka yhteistyöhön perustuva uudelleenkonfigurointi tapahtuu ja suoritetaan verkonlaajuisesti. Luottamuksen hallintaa tarvitaan solmujen välillä vaihdetun tiedon asianmukaiseen hallintaan ja arviointiin. [1, kpl 4 s. 1-2]

Kognitiivisen radioverkon sopeutumiseksi dynaamiseen spektriympäristöön kognitiiviset solmut suorittavat spektrinmittauksen, päätöksenteon käytettävistä taajuuksista, spektrin jakamisen ja spektriin mukautumisen. Jokainen toiminto vaikuttaa solmun eri kerroksiin ja siten koko kognitiivisen radioverkon toimintaan. Näiden eri toimintojen vaikutukset OSI-mallin kerroksissa havainnollistetaan kuvassa 8. Taajuushavainnointiprosessi toteutetaan pääasiassa fyysisessä ja siirtokerroksessa, ja se voi tarjota tietoa spektrin saatavuudesta muille toiminnallisille prosesseille ja ylempien kerroksien protokollille. [1, kpl 4 s. 2]



Kuva 8. Kognitiivisen radion toiminta OSI-mallin kerrosten suhteen. [1, kpl 4 s. 2]

Taajuuspäätösprosessi vastaa sopivien kanavien valinnasta havainnointitulosten ja taajuuksien jakamismenettelyjen perusteella. Taajuuspäätösten tulisi myös perustua palvelun laatuoletuksista (QoS, *Quality of Service*) johtuviin käyttäjän (sovelluksen) vaatimuksiin. Jotta sopivat kanavat saadaan allokoitua verkkoon, on solmujen kommunikoitava verkkokerroksen avulla. Taajuuspäätösten tulisi tehdä yhteistyötä myös reititysprotokollan kanssa reitityksen säätämiseksi reititysmittarien perusteella. Reititysmittarit on laskettu linkin ominaisuuksien perusteella. Taajuuksien jakamisprosessi vastaa resurssien allokoinnista verkossa, jotta vältetään taajuuksien päällekkäisyydet ja vähennetään siten häiriöiden ja päällekkäisyyksien mahdollisuutta. [1, kpl 4 s. 2]

Perinteisillä verkoilla on edelleen haasteita, jotka pysyvät suurimpina esteinä täyden kognition saavuttamiselle koko verkossa. Verkottuneiden toimintojen vertikaalinen integrointi kerrosten välillä, mikä edellyttää kaikkien kerrosten yhteistyötä, on yksi esimerkki näistä haasteista. Kerrosten monimutkaisuudesta johtuen hajautetut ohjausarkkitehtuurit ovat edelleen vaikeuttaneet kognitioita koko verkossa. Yhden haasteen muodostavat valmistajariippuvaiset manuaalisesti konfiguroitavat verkkolaitteet, jotka vaativat käyttäjän toimenpiteitä vaadittuihin muutoksiin. Toisin sanoen SAN-elementit uupuvat ennen ohjelmisto-ohjausta tai sen tärkeintä toteutusta, OpenFlow:ta. [2, s. 21-35]

Koska SDN ratkaisee perinteisiin kerrostettuihin arkkitehtuureihin ja laitekokoonpanoihin liittyviä haasteita, ohjelmisto-ohjatun tietoverkkoarkkitehtuurin ja kognitiivisen verkottumisen käsitteiden yhdistäminen avaa uusia rajoja robustille ja autonomiselle verkon toiminnalle ja hallinnalle. Koska SDN poistaa kognitiivisen tietoliikenneverkon toteuttamisen haasteita, molempien teknisten käsitteiden on oltava integroituna molempien tekniikoiden etujen saavuttamiseksi. Esimerkiksi älykkäät kognitiiviset radiot yhdistettynä mukautuvaan OpenFlow-pohjaiseen verkkoon voivat saavuttaa täysin dynaamiset ja automatisoidut verkkotoiminnot. Tästä huolimatta aihealueesta on vielä hyvin vähän tutkimustietoa, ja saatavilla on vain sovellettavuudeltaan rajoittuneita ehdotuksia ja arkkitehtuurikonsepteja. [2, s. 21-35]

Kognitiiviset verkot vaativat konfiguroitavia verkkoelementtejä, joita voidaan muokata reaaliaikaisesti. Kognitiivisissa verkoissa verkon muutokset voivat johtua solmujen toimintataajuuden muutoksista niiden fyysisen liikkuvuuden lisäksi. Samoin kognitiivisten radioiden on tiedettävä naapuriensa aktiivisuus, niiden sen hetkinen toimintakyky sekä verkon topologia ja parametrit. Nämä tiedot välitetään ylimääräisen, varsinaisten taajuuskanavien välillä hypyttävän ohjaussignaalin avulla. Tämän vuoksi reititystaulukoiden on sisällytettävä myös kontekstikohtaiset tiedot, kuten taajuusparametrit, verkon levittämisparametrit, linkin laadun indikaattorit ja päästä-päähän -suoritusmittarit. Perinteisissä verkoissa nämä ominaisuudet vaatisivat voimakasta vuorovaikutusta eri kerrosten välillä. Eristettyjen kerrosten välinen vuorovaikutus ei kuitenkaan vain lisää koko verkon kompleksisuutta, vaan on myös erittäin haastava järjestelmän kokonaiskustannusten kannalta. Lisäksi toistuva taajuushypytys vaatii erittäin nopeaa uudelleenreititystä. Eri verkkokerrosten rajat ylittävät suunnitteluarkkitehtuurit fyysisen ja johtavat usein epäoptimaaliseen suorituskykyyn verkkokerrosten välisen toistuvan vuorovaikutuksen johdosta. Lisäksi tietoturvahaavoittuvuuksien, kuten väärentämisen, kanssa kerrosten välinen vuorovaikutus voi kaataa koko verkon. Siksi tarvitaan uusia verkkoteknologioita tai konsepteja, jotka voivat ratkaista nämä haasteet. [2, s. 33-34]

2.3.3 Kognitiivinen mobiili Ad hoc-radioverkko (CRAHN - *cognitive radio ad hoc network*)

Langattomat ad hoc -verkot käyttävät laajaa valikoimaa eri reititysprotokollia, jotka rakentavat tyypillisiä reititystaulukoita vain seuraavan hypyn tietojen pohjalta. Suurin osa niistä perustuu joillain muutoksilla varustettuihin OLSR- tai reaktiiviseen AODV-protokollaan (*Optimized Link State Routing, Ad hoc On-Demand Distance Vector Routing*) niiden mukauttamiseksi tiettyyn langattomaan ympäristöön. [1, kpl 4 s. 3] Näitä muutoksia on esimerkiksi ETX-menetelmän (*Expected Transmission Count*) käyttö hyppyjen lukumäärän summaamisen sijaan OLSR-protokollassa. Tämä mahdollistaa reitityksen korkeimman lähetyslaadun perusteella lyhimmän reitin sijasta, sillä hyppyjen lukumäärä ei kerro solmujen välisistä radiotien laaduista tai niiden luotettavuudesta riittävästi. [18, s. 28] Jotkut reititysprotokollat käyttävät maantieteellisiä sijainteja parhaiden reittien löytämiseksi ja valitsemiseksi. Erilaisia reititysratkaisuja voidaan käyttää kognitiivisen radioverkon verkkokerroksessa, mutta niiden tehokkuutta voidaan parantaa käyttämällä muiden kerrosten tietoja. [1, kpl 4 s. 3]

On myös olemassa joitakin protokollaehdotuksia, jotka on jo räätälöity tietyille kognitiivisille radioverkoille. Ne eivät useinkaan täytä sotilaallisia vaatimuksia luotettavan siirtoreitin (tai monikanavaisen siirtoreitin) valinnan ja kognitiivisen kokonaisuuden tuottaman tietoon pohjautuvan reaktion tehokkuuden suhteen. Vain harva tutkituista ratkaisuista perustuu sotilaallisessa käytössä laajasti hyödynnettyihin TDMA-pohjaisiin radioihin, koska ne ovat harvinaisia siviilipuolella. Siksi olisikin tärkeää ehdottaa sellaisten tutkimusmittarien käyttöä, jotka ovat sotilaallisen kognitiivisen radioverkon kannalta merkityksellisiä, ja joita voitaisiin tehokkaasti myös mitata. Tätä varten NATO:n tutkimusryhmä on esittänyt käsitteen CRAHN - kognitiivinen mobiili Ad Hoc-radioverkko. [1, kpl 4 s. 3]

Monet MANET-reititysprotokollat perustuvat lyhyimmän reitin reititysmenetelmiin, mutta se ei ole riittävä CRAHN:ssa. Erittäin suosittu ETX-menetelmä voi reagoida linkin laatuun, mutta sen tarkkuus riippuu tietyn linkin kautta vaihdetusta tosiasiallisesta liikenteestä. NATO:n tutkimusryhmä on esittänyt erityisesti CRAHN-solmuille suunniteltuja protokollia. Tällä hetkellä nämä protokollat ottavat huomioon seuraavat reititysmittarit: [1, kpl 4 s. 3]

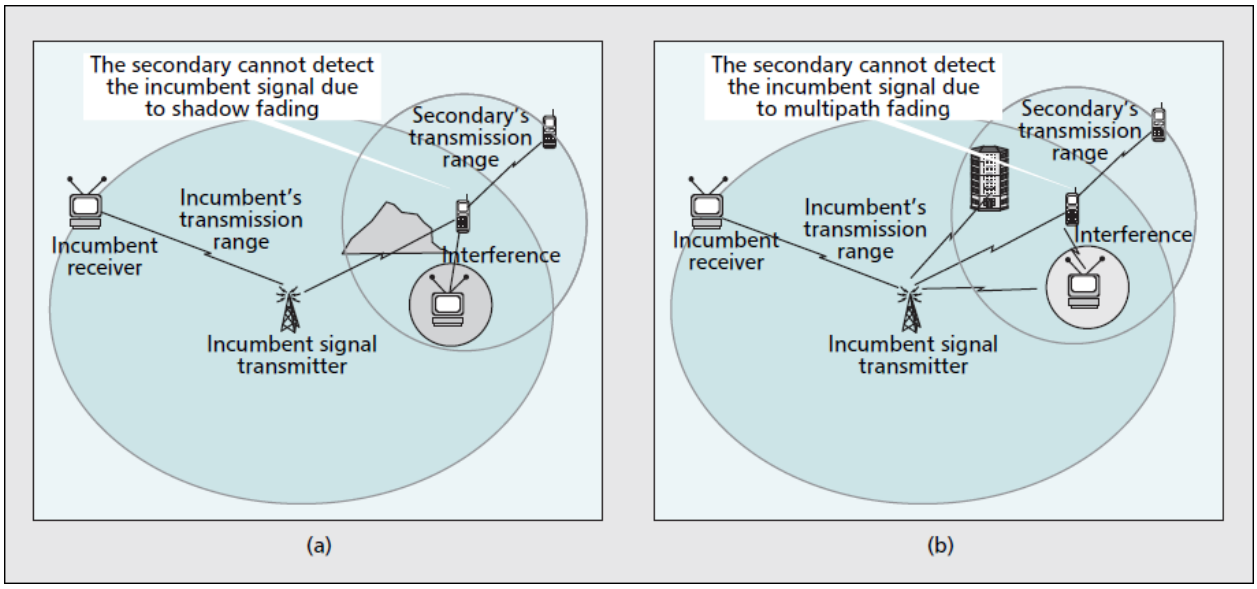
- hyppyjen määrä
- kokonaisviive
- energia
- kaistanleveys
- reitin vakaus
- linkin ja reitin laatu
- kumulatiiviset mittarit

Edellisten lisäksi CRAHN:n reititysprotokollassa tulisi ottaa huomioon ensisijaisen käyttäjän aktiivisuus, samoin kuin tunnistettu multi-hop- ja monikanavainen viestiliikenne.

2.3.4 Jaettu taajuushavainnointi

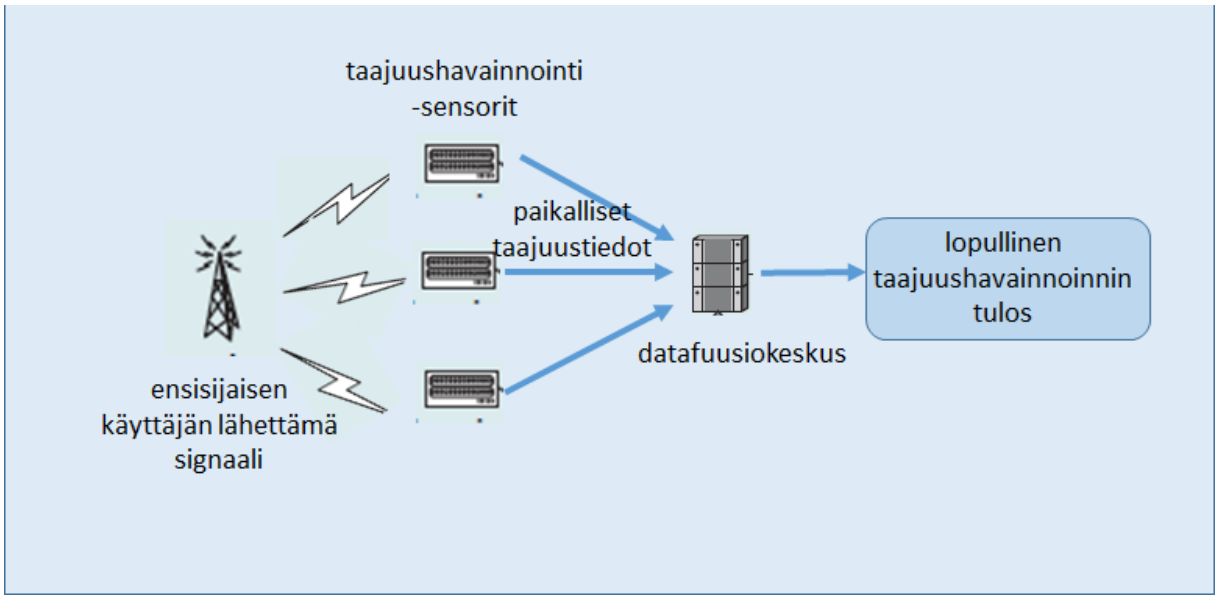
Luotettavan taajuushavainnoinnin suorittaminen on haastava tehtävä kognitiiviselle radiolle. Langattomassa tiedonsiirrossa signaalin häipyminen voi aiheuttaa vastaanotetun signaalin voimakkuuden olevan huomattavasti pienempi, kuin mitä häviömallit ennustavat. Häipymistä on kahta tyyppiä: hidasta häipymistä ja nopeaa häipymistä. Hitaassa häipymisessä esimerkiksi maaston aiheuttamat esteet muuttavat vastaanotetun signaalin keskiarvoa. Hidas häipyminen on taajuusriippumatonta, eikä se aiheuta merkittäviä heilahteluita signaalin voimakkuudessa vastaanottimen sijainnin muuttuessa. Häipyminen on hidasta, mikäli symbolinopeus siirtotiellä on suurempi kuin häipymisen taajuus. [10]

Nopea häipyminen syntyy, kun vastaanottimella summautuu useaa eri reittiä saapunut signaali (monitie-eteneminen). Summautumista kutsutaan interferenssiksi. Nopea häipyminen on taajuusriippuvaista ja voi vaihdella merkittävästi pienillä sijainnin muutoksilla. Nopeaa häipymistä aiheuttavat lähettimen liike ja radioaallon monitie-eteneminen, joiden seurauksena vastaanottimella summautuvien signaalien vaiheet jakautuvat lähes satunnaisesti. Häipyminen on nopeaa, jos symbolinopeus on pienempi kuin häipymisen taajuus. Häipymisen vaikutus voi johtaa niin sanottuun piilotetun solmun ongelmaan. Piilotetun solmun ongelma kognitiivisten radioverkkojen yhteydessä voidaan havainnollistaa esimerkillä, jossa kognitiivisen radioverkon toisiokäyttäjä (*secondary*) on toimivan ensisijaisen käyttäjän (*incumbent*) kantaman sisällä, mutta ei pysty tunnistamaan ensisijaisen käyttäjän olemassaoloa. Kuva 9 havainnollistaa kaksi skenaariota, joissa piilotetun solmun ongelma voi ilmetä. [10]



Kuva 9. Signaalin häipymisestä johtuva piilotetun solmun ongelma [10]

Viimeaikaiset tutkimustulokset osoittavat, että piilotettujen solmujen ongelmaa voidaan vähentää vaatimalla useita toisiokäyttäjiä toimimaan yhteistyössä toistensa kanssa taajuushavainnoinnissa. Tätä kutsutaan hajautetuksi taajuushavainnoinniksi (DSS, *distributed spectrum sensing*). Artikkelissa [14] esitetään kognitiivisista radioista muodostuvan verkon infrastruktuuripohjainen malli. Tässä mallissa jokainen verkon kognitiivinen radio välittää prosessoidut havaintonsa keskusyksikölle, jota kutsutaan fuusiokeskukseksi (FC, *fusion centre*). Fuusiokeskus tekee sitten lopullisen päätöksen ympäristön tilasta jokaiselta kognitiiviselta radiolta kerätyn tiedon pohjalta. DSS:n toimintaperiaate on esitetty kuvassa 10. [10; 14]



Kuva 10. Hajautetun taajuushavainnoinnin toimintaperiaate [10]

DSS:ssä jokainen toisiokäyttäjä toimii siis anturina, joka kerää paikallista taajuusdataa. Fuusiokeskus tekee päätöksen spektrianalyysista kaiken kerätyn datan pohjalta. Kognitiivisessa Ad hoc -verkossa, jossa jokainen solmu toimii toisiokäyttäjänä ja on varustettu kognitiivisella radiolla, solmut toimivat sekä anturipäätteenä että fuusiokeskuksena. Solmu lähettää paikalliset mittaustuloksensa naapureilleen ja suorittaa datafuusion naapureiltaan vastaanottamiensa mittaustulosten avulla. [10; 14]

Yksi DSS:n etu verrattuna yksittäisen päätelaitteen spektrianturiin on sen kyky vähentää spektrin havaitsemisprosessin varianssia. Lisäksi piilotetun solmun ongelman ratkaisemiseksi yhdellä kognitiivisella radiolla tulisi olla riittävän korkea vastaanottimen herkkyys erittäinkin heikkojen ensisijaisten käyttäjien signaalien havaitsemiseksi. Tällaisten erittäin herkkien päätelaitteiden korkeat kustannukset voivat rajoittaa kognitiivisten verkkojen laajempaa käyttöönottoa. DSS mahdollistaakin ensisijaisten käyttäjien signaalin havaitsemisen edullisilla, alhaisen herkkyyden kognitiivisilla radioilla. [10]

DSS:llä on kuitenkin omat heikkoutensa: DSS muodostaa verkossa pullonkaulan vaihtaessaan spektrianturidataa, ja se vaatii luotettavat tietoliikenneyhteydet anturipäätelaitteiden ja fuusiokeskuksen välillä. Vaikka taajuushavainnointi on aktiivinen tutkimusalue, kaikkia turvallisuusnäkökulmia ei ole vielä tutkittu. Taajuushavainnoinnin turvallisuus on ratkaistava, ennen kuin kognitiiviradiotekniikan mahdollistamat hyödyt voidaan hyödyntää täysimääräisesti. [10] Kappaleessa 3.5 käsitellään kahta tietoturvauhkaa DSS:lle kognitiivisissa radioverkoissa. Hyökkäysten analysoinnin jälkeen kappaleessa 3.5 käsitellään myös mahdollisia turvallisuutta parantavia toteutusvaihtoehtoja.

2.4. Kognitiivisen tietoliikennejärjestelmän hyödyt ja haasteet sotilaallisessa kontekstissa

Koska taktisella tasolla tietoliikenneyhteydet ovat tyypillisesti toteutettu radioyhteyksillä, mikä mahdollistaa johtamisjärjestelmän käytön ja tiedon jakamisen myös liikkeen aikana, on verkon muutokset oltava helppo toteuttaa. Kognitiivinen taktinen radioverkko muodostuu kognitiivisista radioista ja verkon suorituskykylisä perustuu radion kykyyn hyödyntää sähkömagneettista spektriä mahdollisimman tehokkaasti. Kognitiivinen taktinen radioverkko on johtamisjärjestelmäkonsepti, jossa langattomat solmut säätävät ominaisuuksiaan ja asetuksiaan saavuttaakseen mahdollisimman tehokkaan ajallisen ja paikallisen spektrinkäytön. [3, s. 23]

Jo pelkästään kognitiivista radiota tarkastelemalla tulee sillä olemaan merkittävä rooli elektronisen sodankäynnin suhteen. Binäärisen automaatiologiikan takia järjestelmän toimintaa on vaikea ennakoida erityisesti tilanteissa, joissa molemmilla osapuolilla on kognitiivisia ominaisuuksia johtamisjärjestelmissään. Kaupallisissa sovelluksissa tuotetestaus on hallittavissa jo tuotekehityksen eri vaiheissa, mutta sotilaallisessa toimintaympäristössä vastapuolten järjestelmien yhtäaikaista toimintaa ei voida etukäteen testata tai edes kaikkea suorituskykyä tuntea. [9, s. 99]

Häirintäjärjestelmien käytössä kognitiivisia radioita vastaan voidaan spektriin esimerkiksi luoda tilanteita, joihin kognitiivisen radion halutaan reagoivan halutulla tavalla. Suojautumisen näkökulmasta näihin erilaisiin tilanteisiin tulee varautua etukäteen esimerkiksi simuloimalla ja mallintamalla häirintä- ja häiriöskenaarioiden vaikutuksia kognitiivisen radion eri toimintatapamalleissa. [9, s. 99] Tästä syystä korostuu jo rauhan aikana saadut vastapuolen järjestelmäkirjastot ja parametrien ja toimintatapojen tuntemus ohjelmoitaessa omaa järjestelmää. Kriisitilanteessa tulisi olla nopea reagointikyky vastapuolen ennalta odottamattomien järjestelmien suorituskykyjen varalta ja niihin liittyen korjaavat toimenpiteet ja päivitykset pitäisi kyetä saamaan joukoille mahdollisimman nopeasti.

Koska taktisella tasalla tietoliikenneyhteydet on toteutettu pääosin langattomin yhteyksin, se voi aiheuttaa ruuhkautuneita ja toisinaan epäluotettavia yhteyksiä. Oman lisähaasteensa langattomiin taktisiin verkkoihin aiheuttaa vihollisen mahdollinen elektroninen häirintä. Näistä syistä johtuen SDN:n kaltainen ohjausarkkitehtuuri ei aina ole sopiva tai mahdollinen. Sotilaallisessa ja taktisessa kontekstissa ei saisi muodostua riippuvuutta yhden pisteen vikaantumiselle (*single point of failure, SPoF*), jota edustaa SDN:n yksi hallittu arkkitehtuuri. Yhtenä mahdollisuutena on hajautetut arkkitehtuurit, mutta ne ovat yleensä käyttökelpoisempia datasentrisissä käyttökohteissa, koska hajautettu arkkitehtuuri aiheuttaa myös suuren tiedonjakoresurssien tarpeen. [19]

Ohjelmisto-ohjatun tietoverkon suunnittelun periaatteina ja etuina pidetään skaalautuvuutta, mukautuvuutta ja helppoa hallinnoitavuutta. Asevoimien kiinteissä ja liikkuvissa taktisissa verkoissa tarpeet ja tilanteet muuttuvat nopeasti, etenkin siirryttäessä normaalioloista poikkeusoloihin. Tällöin ohjelmisto-ohjattua tietoverkkoa voidaan hallita yksityiskohtaisesti istunto-, käyttäjä-, laite- ja sovellustasoilla ja resursseja voidaan jakaa tarvitsijoille nopeasti. Hankenäkökulmasta ja arkkitehtuurin kokonaishallinnan puolesta ohjelmisto-ohjattu tietoverkko ei ole sidottu verkkolaitteiden valmistajien tarjoamiin laiteominaisuuksiin, vaan verkkoa rakennetaan ohjelmistojen avulla. Riittää, että verkkolaite toteuttaa jotakin arkkitehtuurin viestintäprotokollaa, jotta ohjaimen ja laitteen välinen viestintä onnistuu. [16, kpl 4.4]

Yksi erityispiirre tietoliikenteessä sotilasverkoissa on tietoturvaluokitellut tiedot. Siksi ohjelmisto-ohjattuja verkkoja on tutkittu sotilasverkkojen tietoturvan parantamisen näkökulmasta, jolloin sekä liikenteen sisällön salaus kuin myös liikenteen reitityskin tulisi suojatuksi. Molemmat ovat varteenotettavia näkökulmia myös kyberpuolustuksen näkökulmasta. Tietoturvan parantamisen ohella ohjelmisto-ohjattuja verkkoja on tutkittu taktisen verkon tietoliikennesolmujen hallintaratkaisuna autentikoinnin, pääsynhallinnan ja eri liikennöintitarpeiden palvelunlaadun näkökulmista. [16, kpl 4.4]

Nykyaikaisessa sodankäynnissä ja erityisesti kriisinhallinnassa osapuolina on usein monikansallisia joukkoja, mistä aiheutuu myös haasteita tietoliikenneverkkojen kompleksisuudesta johtuen. Koska tietoliikenneverkot ovat usein myös hyvin liikkuvia, verkkotopologia on jatkuvan muutoksen alla eikä vakaata verkkotopologiaa voida taata. Kysymykseksi nouseekin, kykeneekö SDN käsitellä liikkuvan, monia toimijoita sisältävän verkon kompleksisuutta. Lisäksi tietoturvallisuuteen ja puolustukseen liittyvät kysymykset ovat keskeisiä. Mahdollinen yhden pisteen vikaantuminen muodostaa kriittisen uhkan koko verkolle. Jos hyökkääjä onnistuisi murtautumaan järjestelmään ohjaimen kautta, se tekisi koko ohjatun verkko-osan haavoittuvaiseksi. [20]

Teoriassa SDN tarjoaisi kuitenkin monia etuja taktisten verkkojen toiminnalle ja hallinnalle. Näitä ovat mm [20]:

- Parempi, yksityiskohtaisempi ja ketterämpi tietoliikenteen hallinta. Tämä tarkoittaa esimerkiksi ketterämpiä prioriteettisääntöjä verkon ruuhkautuessa tai operatiivisten vaatimusten muuttuessa.

- Verkon dynaaminen sääntöjen hallinta, jotta säännöt voivat paremmin sopeutua paikallisiin olosuhteisiin (tai operaation vaatimuksiin). Säännöt ovat tärkeä tekijä myös kognitiivisten radioverkkojen hallinnassa.

- Jos SDN-ohjaimien liikenteenhallintaa voidaan todellakin laajentaa kohti taktista (langatonta) rajapintaa luotettavalla tavalla, siitä olisi selvää hyötyä luotettavamman ja ”tilannetietoisemman” verkon toiminnan ansiosta.

- Sotilaallisessa toimintaympäristössä tietojärjestelmien päivittäminen on usein hankalaa. Ohjelmisto-ohjatun verkon tietoturva on perinteistä tietoverkkoa helpompi pitää ajan tasalla päivittämällä sovelluksia sen sijaan, että vaihdettaisiin fyysisiä verkkolaitteita tai päivitettäisiin niitä yksittäin. Lisäksi arkkitehtuurissa uusien ominaisuuksien toteuttaminen on nopeampaa. [15, s. 15]

NATO:n tutkimusryhmä [1] on tullut siihen tulokseen, että kiinteiden ja siviiliverkkojen nykyiset verkkoparadigmat eivät välttämättä sovi sotilaallisiin taktisiin radioverkkoihin. Nämä paradigmat voivat tosiasiassa olla haitallisia, koska ne eivät usein tue esimerkiksi tyypillisiä armeijan tietoliikennemalleja ja turvallisuusnäkökohtia. Lisäksi ne eivät tarjoa kognitiivisiin radioverkkoihin tarvittavaa joustavuutta ja mukautettavuutta. Tutkimusryhmä suosittelee seuraavia tietoliikennejärjestelmään liittyviä tekniikoita koskevia ehdotuksia: [1, ES s. 1]

- Reitityksessä tulisi käyttää tekoälyä tai koneoppimistekniikoita reitin valinnan optimoimiseksi.

- Topologian ohjauksessa olisi harkittava yhden linkin sisältämää useiden taajuuksien välistä valintaa. Lisäksi tulee ottaa huomioon erityisesti sotilaalliset näkökulmat, kuten sijaintitietojen turvaluokittelu ja päivittymisen puute radiohiljaisuuden aikana.

- Parannusta olemassa oleviin protokolliin tiedonsiirron tehostamiseksi.

- Klusterointi on tärkeää verkon suunnittelussa. Klusteroinnin tulisi siksi tukea myös muita taktisissa kognitiivisissa radioverkoissa käytettyjä tekniikoita.

- Kontrollikanavan on käsiteltävä voimakkaasti vaihtelevaa tietoliikennemäärää, minkä vuoksi sen tulisi olla mukautettavissa sen hetkiseen liikennemäärään.

Mikäli näihin ehdotuksiin löydetään ratkaisuja, parantavat ne saatavuutta ja päästä päähän -suorituskykyä, koska verkko pystyy paremmin mukautumaan ympäristöönsä. Lisäksi spektrinkäyttö on tehokkaampaa. Verkonhallinta tulisi automatisoida, mikä johtaa vähentyneisiin hallintaponnisteluihin ennen operaatiota, sen aikana ja sen jälkeen. Tämä antaa mahdollisuuden keskittyä entistä enemmän itse tehtävän suorittamiseen. Lisäksi luottamuksen hallinnan tutkimus (käsitelty kappaleessa 3.6) on osoittanut sen merkityksen kontrolliliikenteen eheydelle. Näiden havaintojen perusteella NATO:n tutkimusryhmä ehdottaakin kognitiivisille radioverkoille uutta arkkitehtuurikehystä, jota voidaan pitää lähtökohtana kognitiivisten taktisten radiojärjestelmien standardoinnille ja kehittämiselle. [1, ES s. 2]

Jotta kognitiivisesta tietoliikennejärjestelmästä saataisiin tosiasiallista hyötyä, perusolettamuksena on, että se tarjoaa paremman päästä-päähän -suorituskyvyn kuin perinteinen, ei-kognitiivinen tietoliikennejärjestelmä. Kognitiivisilla prosesseilla voidaan parantaa erityisesti verkon resurssien hallintaa, palvelun laatua, turvallisuutta, kulunvalvontaa sekä pääsynhallintaa. Ideaalitilanteessa toiminta on ennakoivaa, eikä reagoivaa. Tämä asettaakin vaatimuksen, että mukautuminen tapahtuu jo ennen kuin varsinainen ongelma ilmenee. [3, s. 24] Kognitiivisen tietoliikennejärjestelmän hyödyt voidaan kuitenkin hyödyntää vasta silloin, kun järjestelmän suorituskyky ylittää suunnittelusta aiheutuvat kustannukset [2, s. 34].

3. KOGNITIIVISEEN TIETOLIIKENNEJÄRJESTELMÄÄN KOHDISTUVAT KYBERUHKAT JA KYBERTURVALLISUUDEN TOTEUTUSVAIHTOEHDOT

Kognitiivisuus johtamisjärjestelmässä toimii binäärisen logiikan perusteella. Binäärisellä logiikalla tarkoitetaan tietokoneohjelmoitujen radioiden tai radiojärjestelmien toimintaa tilanteessa, jossa molemmat järjestelmät ovat hyvin automatisoituneita. Tästä logiikasta johtuen tätä toimintaa voi olla vaikea ennakoida erityisesti tilanteissa, joissa molemmilla osapuolilla on johtamisjärjestelmissään kognitiivisia ominaisuuksia. Pahimmillaan kognitiivisen radion tai verkon hyödyt voivat juuri niiden automaattisuuden vuoksi kääntyä haitaksi. Pitkälle viety automaattisuus voi olla järjestelmän heikko kohta, jota kohtaan vastustaja pyrkii vaikuttamaan. [9, s. 38]

Monitasoisen verkottumisen vaatimuksena ja ohjelmistopohjaisuuden seurauksena merkittäväksi haasteeksi kognitiivisille radiojärjestelmille voidaan nostaa kyberuhkat kaikissa muodoissaan, joista yleisimmät taktisia verkkoja vastaan ovat: [9, s. 39]

- tiedon eheyden rikkomukset (*integrity violation*)
- tiedon saatavuuden estäminen (*prevention of availability*),
- luottamuksellisuuden rikkomukset (*confidentiality violation*) sekä
- fyysinen tuhoaminen (*kinetic destruction*)

Kaikkia mahdollisia taktisen verkon kyberuhkia ei voida listata tai laatia, koska menetelmät ja työkalut muuttuvat ja kehittyvät koko ajan [21, s. 39–40] Kuten edellisestä listasta havaitaan, kyberuhkat muodostavat laajan ja merkittävän uhkan kognitiivisille radiojärjestelmille. Kyberoperaatioiden mahdollisuudet lähtevät kontrolliliikenteen sieppauksesta aina järjestelmän tietojen varastamiseen. On myös mahdollista, että onnistuneella kyberoperaatiolla tietokannat voidaan tyhjentää ja verkon solmukohdat maalittaa tuhoamista varten. [9, s. 43]

Tässä tutkimuksessa on tuotu esiin erityisesti langattoman, taktisen kognitiivisen tietoliikennejärjestelmän taajuushavainnointiin, hajautettuun tiedonvaihtoon sekä kontrolliliikenteeseen liittyviä haavoittuvuuksia sekä SDN-pohjaisen arkkitehtuurin haavoittuvuuksia. Näihin haavoittuvuuksiin on kartoitettu erilaisia tekniikoita ja toteutusvaihtoehtoja, jotka voisivat mahdollisesti parantaa järjestelmän kyberturvallisuutta ja toimintakykyä.

3.1. Haavoittuvuudet dynaamisessa spektrinkäytössä (DSA)

Dynaaminen spektrinkäyttö (DSA) on lähestymistapa, joka automatisoi taajuuden asettamisprosessin täysin, jolloin radioverkko itse voi määrittää taajuusasetuksensa perustuen taajuushavainnointiin. Sen lisäksi, että DSA:ta käytetään spektrin tehokkaampaan hyödyntämiseen, sitä on esitetty tiedeyhteisössä keinona vähentää elektronisen sodankäynnin tai kyberhyökkäyksen vaikutuksia, koska verkko voi väistää hyökkääjän vaihtamalla taajuusasetuksia. Tämä näkökulma on kuitenkin yksipuolinen ja tulisi ymmärtää, että itse DSA-protokollia voidaan manipuloida, ja että nämä protokollat voivat luottaa epäselviin käyttäjärooleihin ja käyttöoikeuksiin, joita voidaan hyödyntää. Kanadan puolustusvoimien tutkimus- ja kehittämislaitoksen tutkimuksen [22] mukaan DSA-haavoittuvuuksia löytyy protokollien puutteista, jotka mahdollistavat verkon oman taajuuspäätösprosessin manipuloinnin vastustajan etujen mukaisesti. Kaupallisen DSA-radiotekniikan haavoittuvuuksia on tutkittu paljon, mutta DSA:n sotilaallisten toteutusten haavoittuvuuksia ei vielä tunneta hyvin. [22, s. 2]

Mikäli radioverkkoa käytetään automaattisella kanavanvalinnalla, verkon havaitessa nykyisellä kanavalla kynnysarvoa suurempaa häiriötä, se vaihtaa toiseen käytettävissä olevaan kanavaan, jolla on vähemmän häiriöitä. Verkon kanavanvaihto on ennustettavissa, mikäli sen tiedetään olevan DSA-verkko. Vastustaja voi hyödyntää tätä ennustettavuutta. Vastustajan elektroninen häirintä voi myös havaita taajuuksien nykyisen käyttöasteen ja päättää sen perusteella millä kanavalla verkkoa häiritään. Mikäli tätä tehdään toistuvasti, sitä kutsutaan seurantahäirinnäksi (*chaser jammer*). [22, s. 13]

Seurantahäirintä muodostaa merkittävän haavoittuvuuden DSA-verkolle. Toistuvat taajuusvaihdot heikentävät verkon suorituskykyä merkittävästi. Samalla kun yhteyden muodostumista uudelle kanavalle ollaan asettamassa, muodostuu viive, jolloin hyötylähetettä ei voida lähettää koska verkko käyttää resursseja kontrolliliikenteeseen. Verkossa viestit jäävät puskurimuistiin, mutta osa saattaa silti kadota. Kanavan vaihtamisnopeus on rajallinen, mistä syystä verkko kärsii häiriöistä, kunnes se toipuu uudella kanavalla. Verkon ja häirintäaseman suorituskyvystä riippuen, seurantahäirintä voi kokonaan estää palvelut verkossa. [22, s. 13-14]

Väite, että seurantahäirintä DSA-verkossa ei aiheuta suurempaa uhkaa kuin perinteinen häirintälaite perinteisessä verkossa ei pidä paikkansa, sillä se voi tukkia verkon tehokkaammin. Tämä johtuu siitä, että häirintäaseman tarvitsee häiritä tavanomaista häirintää pienemmällä teholla ja vain tietyllä ajanjaksolla. Häirintätehon tarvitsee olla riittävä ylittämään vain häiriökynnyksen ja laukaisemaan kanavanväistötoimenpiteet. Perinteisessä häirinnässä sen sijaan suuremmalla lähetysteholla pyritään kaikkien vastaanottimien ylikuormittamiseen. Lisäksi, koska DSA-radion säteilijässä sekä taajuushavainnointi että lähetys ovat lomittuneina, lyhentää se lähetyksen kokonaisaikaa perinteiseen radioon verrattuna. Siten häirinnän toimintajaksoa voidaan myös lyhentää hyödyntämällä DSA-radion lyhyempää käyttöjaksoa. [22, s. 13-14]

Yhtä lailla DSA luo mahdollisuuden vastustajalle saada käyttäjät valitsemaan tietty taajuuskanava (kanavat) ”laumakäyttäytymisellä”. Vastustaja saattaa tukkia kaikki mahdolliset taajuuskanavat paitsi yhden, jolloin tämä yksi kanava näyttää houkuttelevalta verkolle. Tämä taajuuskanava voi olla kanava, joka on vastustajalle helpoimmin havaittavissa. Vastustaja saattaa haluta myös pakottaa verkon tiettyyn spektrimääritykseen, joka mahdollistaa hyökkäyksen toisen vaiheen käynnistämisen. Vastustaja voi esimerkiksi häiritä verkon tietyn osan kanavia liikenteen ohjaamiseksi kohti tietomurrettua solmua. [22, s. 14]

Mikäli DSA-verkko toteuttaa taajuuksien hallinnassa toiminnon, jolla mahdollistetaan ensisijaisten ja toisiokäyttäjien toimiminen rinnakkain, häirinnällä voi olla myös vakavat vaikutukset. Ellei verkko totea, että häirintälähete on läsnä, toisiokäyttäjien on oletettava, että häiriöt johtuvat ensisijaisesta käyttäjästä. Tämä johtaa toisiokäyttäjien spektrin vapauttamiseen, kunnes häiriötä ei enää ole. Tämän jälkeen vastustaja voi tukkia kanavan tai kanavia joko lähettämällä kohinaa, joka ylittää vain toisiokäyttäjien radioiden havaitsemiskynnyksen, tai lähettämällä ensisijaisen käyttäjän aaltomuotoa jäljittelevän signaalin. Näin toimiessaan vastustaja estää palvelut toisiokäyttäjiltä estämällä niiden spektrin käytön. Toisin sanoen tällainen häirintä vaatii huomattavasti vähemmän lähetystehoa kuin perinteinen häirintä, jossa tehokilpailulla pitää voittaa hyötylähete vastaanottimessa. [22, s. 14] Tällaista hyökkäysmallia kutsutaan myös termillä ensisijaisen käyttäjän emulointihyökkäys (IE, *incumbent emulation* tai *primary user emulation*), jota on käsitelty tarkemmin kappaleessa 3.5.

3.2. Ohjelmisto-ohjatun tietoverkon uhkat

Ohjelmisto-ohjattujen tietoverkkojen tämänhetkinen tutkimustilanne on tunnistanut teoreettisia ja mahdollisia tietoturvauhkia kaikista arkkitehtuurin tasoista ja rajapinnoista. Perusratkaisu erottaa hallinta- ja tiedonvälityskerros toisistaan mm. paremman näkyvyyden, yksinkertaisen verkonhallinnan, johdonmukaisen verkkokäytänteiden valvonnan ja uusien toimintojen käyttöönoton helpottamiseksi ilmenee sekä etuna että uhkana. Samat ominaisuudet voivat tehdä SDN:t erittäin alttiiksi tietoturvauhkille. Esimerkiksi ohjaustason keskittäminen tekee siitä helpon kohteen palvelunestohyökkäykselle (DoS, *Denial of Service*) ja verkon kyllästämishyökkäyksille. [2, s. 36]

Ohjelmoitavilla verkoilla on ollut alttiutta myös tietoturva-aukkoihin. Aktiivinen verkottuminen (*Active Networking*) on yksi näkyvimmistä esimerkeistä ohjelmoitavista verkkoarkkitehtuureista, jota ei käytetä sen turvallisuushaavoittuvuuksien vuoksi. Siksi on erittäin tärkeää tutkia SDN:n turvallisuusuhkia ja yrittää etsiä ratkaisuja näihin haasteisiin. [2, s. 36] SDN-ohjain voi muodostaa houkuttelevan hyökkäysrajapinnan, jonka kautta voidaan päästä käsiksi koko tietoliikennejärjestelmään. Ohjainohjelmisto on alttiina kaikille ohjelmistoille tyypillisille vioille ja puutteille, jotka voivat aiheuttaa tietoturvaongelmia. Arkkitehtuurin hallintatason tietoturvaa voikin siksi pitää erityisen tärkeänä, koska ohjaimen vaarantumisella voi olla vakavat seuraukset koko verkossa. [16, kpl 4.4]

Open Networking Foundation (ONF) on julkaissut SDN:n tietoturvaan liittyen kolme teknistä suositusta: SDN-ohjaimien tietoturvavaatimukset, SDN-arkkitehtuurin uhka-analyysi ja ohjelmistopohjaisten verkkojen turvaamisen periaatteet ja käytännöt [26; 27; 28]. Tutkimuksissa on tunnistettu seitsemän eri tyyppistä uhkakategoriaa, jotka uhkaavat nimenomaan ohjelmisto-ohjattuja tietoverkkoja: [16, kpl 4.4]

- muokatut tai väärennetyt tietovuot
- kytkinten haavoittuvuuksien hyödyntäminen hyökkäyksissä
- kontrollikerroksen viestintään kohdistuvat hyökkäykset
- ohjaimiin ja niiden haavoittuvuuksiin kohdistuvat hyökkäykset
- puutteelliset luottamuksen varmentamismekanismit ohjaimen ja hallintaohjelmiston välillä
- ylläpitolaitteisiin ja niiden haavoittuvuuksiin kohdistuvat hyökkäykset

- luotettavien tutkinta- ja korjausresurssien puute

Ohjelmisto-ohjattujen verkkojen ohjaus- ja hyötyliikenteen erottaminen mahdollistaa uudenlaisia uhkia, kuten *Man-In-The-Middle*-hyökkäykset sekä palvelunestohyökkäykset (DoS, *Denial of Service*). SDN-arkkitehtuurin tietoturvan heikkouksina on tarkasteltu muun muassa ohjaimen pääsynvalvontaa ja valtuutusmenetelmiä, ohjaimeen kohdistuvia palvelunestohyökkäyksiä, ohjaimen identiteettivarkauksia sekä avoimiin protokolliin ja rajapintoihin kohdistuvia uhkia. [16, kpl 4.4]

SDN-arkkitehtuurin tietoturvallisuutta on myös standardoitu; kansainvälisen televiestintäliiton standardointiosasto (ITU-T) on laatinut omat suosituksensa arkkitehtuurin tietoturvan parantamiseksi [23], samoin myös IEEE Standards Association kehittää omaa standardiaan [24]. Taulukossa 1 on esitelty ITU-T:n tunnistamia ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhkia tasojen ja rajapintojen mukaan luokiteltuna. ITU-T on antanut myös suosituksensa uhkien ehkäisemiseksi.

Uhka	**Kuvaus**
Verkkosovellustaso	
Väärentäminen	Hyökkääjä esiintyy ohjaimena.
Kiistäminen	Käyttäjä voi toimia haitallisesti ja kieltää tekonsa.
Tiedon paljastuminen	Hyökkääjä voi käyttää oikean käyttäjän tunnuksia ja lähettää verkkoon väärennettyä liikennettä verkkosovelluksen kautta.
Verkkosovellusten haavoittuvuudet	Hyökkääjä voi päästä käsiksi sovelluksen resursseihin ja käyttää niitä muissa hyökkäyksissä.
Hallintataso	
Vuosääntöjen ristiriidat	Verkkosovellus voi korvata toisen sovelluksen antaman vuosäännön.
Haitallinen vuosääntö	Hyökkääjä voi kaapata verkkosovelluksen ja asentaa haitallisen vuosäännön salakuunnellakseen tietoja.
Väärentäminen	Hyökkääjä voi esiintyä pääkäyttäjänä tai verkkosovelluksena ja muokata tai poistaa tietoja, käsitellä topologia- ja reititystietoja tai saada koko ohjaimen haltuunsa.

	Väärentämällä ohjaimen osoitteen hyökkääjä voi käyttää verkossa omaa ohjaintansa. Hyökkääjä voi luoda kytkimen ja saada tietoja verkosta tarkkailemalla, miten ohjain reagoi erilaisiin paketteihin.
Palvelunestohyökkäys Viive hyökkäyksen torjunnassa	Hyökkääjä voi luoda liikennettä, joka saa kytkimen kysymään ohjaimelta vuosääntöjä ja näin kuormittaa ohjainta. Vuosääntöjä päivitetään tavallisesti tietyin väliajoin suorituskyvyn parantamiseksi, jolloin kiireelliset päivitykset hyökkäyksen pysäyttämiseksi viivästyvät.
Kiistäminen	Pääkäyttäjä tai verkkosovellus voi asentaa haitallisia vuosääntöjä ja kiistää tekonsa.
Tiedon paljastuminen	Hyökkääjä voi saada haltuunsa tietoja järjestelmästä tulevaa hyökkäystä varten.
Käyttöjärjestelmän haavoittuvuudet	Ohjainohjelmistoa ajetaan jossain käyttöjärjestelmässä, jolloin käyttöjärjestelmän haavoittuvuudet ovat myös ohjaimen haavoittuvuuksia.
Ohjelmiston haavoittuvuudet	Hyökkääjä voi hyödyntää virheitä, puutteita ja heikkouksia ohjainohjelmistossa hyökkäyksissään.
Laitteistoviat	Ohjaimen tai kytkinten laitteistoviat voivat vaarantaa turvallisuuden tai kaataa verkon.
Verkkoelementtitaso	
Väärentäminen	Hyökkääjä voi esiintyä pääkäyttäjänä tai ohjaimena päästäkseen käsiksi kytkimen tietoihin.
Salakuuntelu	Hyökkääjä voi salakuunnella kytkinten välistä liikennettä ja saada tietää, millaista tietoa verkossa liikkuu, mikä liikenne on sallittua ja millaisia voita on käytössä.
Tiedon paljastuminen	Hyökkääjä voi saada haltuunsa tietoja järjestelmästä tulevaa hyökkäystä varten.
Vuotaulun ylivuoto	Kytkimellä on tavallisesti rajallinen vuotaulu, jota hyökkääjä voi hyödyntää oikeiden vuosääntöjen ylikirjoittamisessa tai palvelunestohyökkäyksessä.
Kiistäminen	Pääkäyttäjä tai ohjain voi muuttaa laitteen asetuksia ja kiistää tekonsa.
Verkkosovellus- ja hallintatason rajapinta	

Salakuuntelu	Salakuunneltujen tietojen perusteella hyökkääjä voi päätellä verkon käytäntöjä ja hyödyntää niitä hyökkäyksissä.
Viestien muuttaminen ja sieppaaminen	Hyökkääjä voi siepata tai muuttaa ohjaimen ja sovelluksen välisiä viestejä esimerkiksi käytäntöjen muuttamiseksi.
Hallinta- ja verkkoelementtitason rajapinta	
Salakuuntelu	Hyökkääjä voi salakuunnella ohjaimen ja kytkimen välisiä viestejä ja päätellä verkon reitityskäytännöt.
Viestien muuttaminen ja sieppaaminen	Hyökkääjä voi siepata tai muuttaa ohjaimen ja kytkimen välisiä viestejä esimerkiksi lähettääkseen omia viestejä kytkimille.

Taulukko 1: Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhkia [23]

Ahmad [2] on väitöskirjassaan laatinut vastaavan, yksityiskohtaisemman listauksen ohjelmisto-ohjattua tietoverkkoarkkitehtuuria vastaan kohdistuvista uhkista, joista on koonnos taulukossa 2. Ymmärrettävyyden lisäämiseksi turvallisuushaasteet ja ratkaisut voidaan kuvata jokaiselle kolmelle SDN-tasolle ja niiden välisille rajapinnoille. Verkkosovellus- ja hallintatasojen välistä rajapintaa kutsutaan *northbound-API*:ksi, ja hallinta- ja verkkoelementtitasojen välistä rajapintaa vstaavasti *southbound-API*:ksi. [2, s. 36]

Uhka	**Kuvaus**
Verkkosovellustaso	
Autentikoinnin ja valtuutusten puuttuminen	Sovellusten todentamis- ja valtuutusmekanismien puuttuminen aiheuttaa vielä suuremman uhkan, jos kyseessä on suuri määrä kolmansien osapuolten sovelluksia.
Vuosääntöjen väärentäminen	Haitalliset tai saastuneet sovellukset voivat luoda vuosääntöjä. Saastuneen ohjelman löytäminen on vaikeaa.
Käytönvalvonnan ja -vastuun puuttuminen	Vaikea toteuttaa pääsynhallintaa ja vastuuvelvollisuutta kolmansien osapuolten sovelluksissa ja sisäkkäisissä sovelluksissa, jotka kuluttavat verkkoresursseja.

Hallintataso	
Palvelunestohyökkäys	Verkon näkyvyys, keskitetty älykkyys ja rajalliset resurssit ovat tärkeimmät syyt hallintatason palvelunestohyökkäyksille.
Ohjaimen luvaton käyttö	Ei pakottavia mekanismeja pääsyn valvonnan varmistamiseksi sovelluksissa.
Skaalautuvuus ja saatavuus	Älykkyyden keskittäminen yhteen kokonaisuuteen todennäköisesti lisää skaalautuvuuden ja saatavuuden haasteita.
Verkkoelementtitaso	
Väärennetyt vuosäännöt	Verkkoelementtitaso on ”tyhmä” ja siten altis vuosääntöjen väärentämiselle.
Tulvitushyökkäys	OpenFlow-kytkimien vuotaulukoihin voidaan tallentaa rajallinen tai rajoitettu määrä vuosääntöjä.
Ohjaimen kaappaus tai vaarantuminen	Verkkoelementtitaso on täysin riippuvainen hallintatasosta, mikä tekee verkkoelementtitason turvallisuudesta riippuvaisen ohjaimen turvallisuudesta.
TCP-hyökkäykset	TLS on altis TCP-tason hyökkäyksille.
Man-in-the-middle -hyökkäykset	Tämä johtuu TLS:n valinnaisuudesta, sekä TLS:n konfiguroinnin monimutkaisuudesta.

Taulukko 2. Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tasoittain luokitellut uhkat ja niiden kuvaukset [2]

3.2.1 Verkkosovellustason tietoturvahaasteet

Kuten aiemmin on kuvattu, verkkosovellukset toteuttavat suurimman osan verkkotoiminnoista olematta sidottuja itse verkkoon. Siksi sovellusten turvallisuudella on suuret vaikutukset. Sovellukset on todennettava ja varmennettava ennen vuosääntöjen luomista. Ohjaimen ja sovellusten välillä ei kuitenkaan ole vakiintuneita varmennemekanismeja. Eri sovelluksilla on erilaiset käyttöoikeudet, joten sovellusten eristämiseen on asetettava tietoturvamalli. Tässäkään tapauksessa ei ole olemassa pakottavia mekanismeja, jotka tarjoaisivat eriytetyn pääsyn sovelluksille heidän käyttöoikeuksiensa perusteella. Haastetta monimutkaistaa edelleen sisäkkäiset sovellukset, joissa haitallisten sovellusten seuraaminen laillisten sovellusten sisällä on erittäin haastavaa. Sisäkkäisten sovellusten vastuuvelvollisuutta ei myöskään ole määritelty. [2, s. 36-37]

3.2.2 Hallintatason tietoturvahaasteet

SDN-ohjaimen on todennettava sovellukset ennen verkkotietojen tarjoamista sovelluksille. Ohjaimessa on kuitenkin itsessään monia turvallisuushaasteita. Verkko-ohjauksen keskittäminen ohjaimeen tarkoittaa valtavaa lukumäärää sovelluksia ja niiden alla olevia ohjattavia laitteita. Tämä voi tehdä ohjaimesta potentiaalisen pullonkaulan skaalautuvuuden tai resurssirajoitusten vuoksi. Tämä skaalautuvuusrajoitus avaa ovet palvelunestohyökkäyksille. Verkon tunnistusmenetelmiä on mahdollista käyttää verkon tunnistamiseksi SDN:ksi ja hyökkäyksen käynnistämiseksi. Tietäen, että kytkimen on lähetettävä tietovuon asetuspyyntö ohjaimelle jokaista uutta tietovuota varten, palvelunestohyökkäys voidaan kohdistaa helposti ohjaimeen. Yhteenvetona voidaan todeta, että ohjain on toisaalta SDN:n tärkein, ja toisaalta myös haavoittuvin osa palvelunesto- ja hajautettujen palvelunestohyökkäysten takia. [2, s. 37]

3.2.3 Verkkoelementtitason tietoturvahaasteet

Verkkoelementtitasolla, kuten esimerkiksi OpenFlow-kytkimissä, tietovuot tallennetaan sen jälkeen, kun ensimmäinen paketti on lähetetty ohjaimelle vuosääntöjen asettamiseksi. Vuotaulukoilla, jotka ylläpitävät vuosääntöjä sekä puskurilla, joka tallentaa ei-toivotut tietovuot, on rajoittunut fyysisen kapasiteetti. Tätä rajoittuneisuutta voidaan hyödyntää myös palvelunestohyökkäyksen käynnistämiseksi OpenFlow-kytkimiä vastaan. Lisäksi verkkolaitteet ovat SDN:ssä yksinkertaisia ja erittäin riippuvaisia ohjaimesta. Tämä tarkoittaa, että verkkolaitteilla ei ole kykyä erottaa aitoja ja virheellisiä tai haitallisia vuosääntöjä. Samoin jos ohjain vaarantuu, epäonnistuu tai yhteys ohjaimeen katkeaa, verkkoelementtitaso vaarantuu tai ei kykene vastaamaan saapuviin tietovoihin. [2, s. 37-38]

3.2.4 Rajapintojen tietoturvahaasteet

OpenFlow-kytkimen määritelmä ehdottaa TLS- (*Transport Layer Security*) ja DTLS-salausprotokollia (*Datagram Transport Layer Security*) southbound-API:n, esimerkiksi OpenFlow-protokollan suojaamiseen. TLS ei ole kuitenkaan standardilla määritelty, ja tämä suojausominaisuus jätetään vain valinnaiseksi. TLS:n valinnainen käyttö jättää ohjauskanavan ohjaimien ja kytkinten välillä avoimiksi tietoturvauhkille, kuten man-in-the-middle -hyökkäyksille ja väärennettyjen sääntöjen lisäyksille. Lisäksi TLS-salausprotokolla on erittäin monimutkainen, mikä tekee sen käytöstä teknisen haasteen verkonhallinnassa. Siksi southbound-API:n turvallisuus SDN:ssä on edelleen tutkimushaasteena. Northbound-API:lla sitä vastoin ei ole nimenomaisesti määriteltyjä tietoturva-arkkitehtuureja. Toisin sanoen etäsovellusten ja ohjaimen välistä kommunikointia ei ole edes tutkittu kunnolla. [2, s. 38]

3.2.5 Palvelunestohyökkäys ohjelmisto-ohjatussa tietoverkossa

Palvelunestohyökkäyksen perusperiaatteena on, että hyökkääjä lähettää palvelimelle niin paljon dataa, että oikeat käyttäjät eivät voi hyödyntää palvelua. Hajautetut palvelunestohyökkäykset (DDoS, *Distributed Denial-of-Service*) ovat vieläkin vaikeampia ehkäistä ja torjua. [15, s. 25]. Qiao et al. [25] mukaan kaikki ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tasot ja rajapinnat ovat alttiita palvelunestohyökkäyksille. Koska ohjaimen turvallisuus on erityisen kriittinen verkon toiminnan kannalta, muodostaa se houkuttelevan kohteen palvelunestohyökkäykselle. Toisaalta ohjelmisto-ohjattua arkkitehtuuria voidaan käyttää myös hyväksi hyökkäyksiltä suojautumisessa. [25] Tämä johtuu siitä, että ohjelmisto-ohjatussa tietoverkossa reitityssääntöjä voidaan asentaa kytkimiin myös tarvittaessa (reaktiivisesti). Reaktiivista vuosääntöjen luomista voidaan hyödyntää palvelunestohyökkäyksissä. Esimerkiksi kytkimen vastaanottaessa paketin, jota se ei osaa reitittää, se tallentaa paketin puskuriinsa ja lähettää paketin tiedot ohjaimelle. Ohjain lähettää kytkimelle uuden vuosäännön, jonka mukaan kytkin voi reitittää kyseisen vuon paketit tulevaisuudessa. [15, s. 27]

Siironen [15] on tunnistanut pro gradu -tutkielmassaan kolme erilaista vaikutusmekanismia palvelunestohyökkäyksille SDN-verkoissa. Hyökkäystavat ja niiden kohde sekä vaikutukset on esitelty taulukossa 3.

Hyökkäys	**Kohderesurssi**	**Vaikutukset**
Suuri määrä uusia voita	Ohjaimen ja kytkimen välinen kaistanleveys	Vaikeuttaa ohjaimen ja kytkimen viestintää.
	Ohjaimen prosessointiteho	Hidastaa ohjaimen toimintaa.
	Kytkimen muisti	Täyttää kytkimen vuosääntötaulua.
Suuri määrä paketteja tuntemattomille vastaanottajille	Ohjaimen ja kytkimen välinen kaistanleveys	Vaikeuttaa ohjaimen ja kytkimen viestintää.
	Ohjaimen prosessointiteho	Hidastaa ohjaimen toimintaa.
	Kytkimen muisti	Täyttää kytkimen pakettipuskuria.
Palvelimen sijainnin kaappaus		Oikea palvelin ei saa sille tarkoitettua liikennettä.

Taulukko 3. Ohjelmisto-ohjatun tietoverkon palvelunestohyökkäyksiä [15, s. 29]

Mikäli ohjelmisto-ohjatussa verkossa on suuri määrä liikennettä, voi se saada kytkimet lähettämään monia paketteja ohjaimelle reitityspäätöstä varten, mikäli niiden reitityssääntöjä ei ole etukäteen lisätty kytkimeen. Tällöin ohjaimen prosessointiteho ei välttämättä riitä, ja liikenne hidastuu kytkinten odottaessa reititysohjeita. Tilannetta voi auttaa ohjaimen hajauttaminen, jolloin kytkimet voidaan jakaa useamman ohjaimen vastuulle. [15, s. 27]

Palvelunestohyökkäys voi myös täyttää kytkimen vuotaulut generoimalla tekaistuja paketteja. Vaikutus perustuu siihen, että ohjain asentaa kytkimeen uuden vuomerkinnän jokaiselle paketille, jonka otsakkeet eroavat edellisistä. Tämä kuluttaa lopulta kytkimen muistin loppuun, eikä uusille vuosäännöille ole enää tilaa. Tätä hyökkäystä vastaan on ehdotettu kahta ratkaisua: joko ohjaimen pitäisi pystyä pitämään verkko toiminnassa kytkimen muistin loppumisesta huolimatta, tai ohjain voisi väliaikaisesti tallentaa vuomerkintöjä itse ja vaihtaa niitä kytkimeen tarpeen mukaan. Muun muassa suositun OpenFlow-protokollan määritelmä sallii kytkinten poistaa vuosääntöjä itsenäisesti. [15, s. 27]

Yksi tapa toteuttaa hajautettu palvelunestohyökkäys on käyttää hyväksi ohjaimen toimintaa, kun sen pitäisi välittää paketti, jota se ei osaa reitittää. Tällöin ohjain antaa jokaiselle kytkimelle käskyn lähettää kyseinen paketti kaikille siihen kytkeytyneille laitteille, jolloin se saattaisi päätyä oikealle vastaanottajalle. Ohjaimen vastaanottaessa suuren määrän tällaisia paketteja verkko kuormittuu laitteiden välittäessä niitä eteenpäin. Tämä hyökkäystapa hyödyntää siis verkkoon jo kuuluvia kytkimiä liikenteen lisäämisessä. Se voi täyttää kytkinten pakettipuskurit, ylikuormittaa ohjainta ja viedä verkon kaistanleveyttä. Tätä hyökkäystä voidaan pitää todellisena uhkana ja suurissa verkoissa sillä on luultavasti vakavat vaikutukset. Hyökkääjän on myös mahdollista esiintyä jonain verkon isäntäkoneena huijaamalla ohjainta luulemaan, että kone on vaihtanut paikkaa verkossa. Jos hyökkääjä voi ohjata jonkun palvelimen liikenteen itselleen, palvelin ei voi palvella sen asiakkaita. [15, s. 28]

3.2.6 SDN-pohjaiset tietoturvaratkaisut

Ohjelmisto-ohjattujen verkkojen alttius hyökkäyksille on kaksijakoinen, sillä kyky liikenneanalyysiin, loogisesti keskitetty ohjaus, verkon kokonaistilanteen havainnointi sekä reititystaulujen dynaaminen päivitys mahdollistavat myös hyökkäysten havaitsemisen sekä vastatoimenpiteet. Tietoturvaa onkin pyritty parantamaan ohjelmoitavilla tietoverkoilla jo pitkään. Esimerkki mahdollisesta puolustuksellisesta vastatoimenpiteestä voisi olla palvelunestoliikenteen dynaaminen ohjaus esimerkiksi niin sanottuun hunajapurkkiin hyökkäyksen analysoimiseksi. [16, kpl 4.4]

OpenFlow-toteutuksen edeltäjässä, Ethane-arkkitehtuurissa, on loogisesti keskitetty ohjain, joka hallitsee yksinkertaisia kytkimiä. Tietoturvallisuus on toteutettu kiinteänä osana arkkitehtuuria esimerkiksi pääsynhallinnan muodossa. Ethane myös sitoo paketin ja sen lähettäjän tiukasti yhteen, jolloin käyttäjien seuraaminen on mahdollista, vaikka sijainnit muuttuisivatkin. Ohjelmisto-ohjatussa tietoverkossa turvallisuutta ei ole suunniteltu osaksi arkkitehtuuria, joten Ethanen tietoturvan toteutuksesta voitaisiin ottaa opiksi ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa. [15, s. 14-15]

Kytkimen vuotaulukot sisältävät myös muita tietoja tietovoista, kuten mm. pakettilaskurin arvot sekä aikakatkaisuarvot, jotka ovat aina ohjaimelle näkyvissä. Ohjainta käyttämällä SDN-sovellukset voivat pyytää vuo-ominaisuuksia, kuten aikakatkaisuarvoja tai pakettinäytteitä, ja käyttää niitä verkon muunteluun luomalla uusia vuosääntöjä. Tällainen sääntö voi olla esimerkiksi tiettyjen pakettien edelleen lähettäminen tietyille porteille. Päätöstä tiettyjen pakettien edelleen lähettämisestä tietyille porteille voidaan tarvita silloin, kun kuormitusta tulee tasapainottaa, tai esimerkiksi turvallisuusanalyysin suorittamiseksi. Kuormituksen tasapainottamisen tapauksessa uudet ulosmenoportit voidaan kytkeä vähemmän kuormitettuihin kytkimiin tai muihin verkkolaitteisiin. Tietoturvallisuuden suhteen uudet ulosmenoportit voidaan kytkeä esimerkiksi palomuureihin tai tunkeutumisen tunnistamisjärjestelmiin (IDS). SDN mahdollistaakin laajan ohjelmistopohjaisen innovoinnin tietoliikenneverkoissa. [2, s. 28]

Ohjelmisto-ohjattujen tietoverkkojen lähikäsitteenä voidaan pitää myös verkkotoimintojen virtualisointia (*Netvork Function Virtualization*, NFV), jolla tarkoitetaan verkkotoimintojen toteutusta ohjelmallisesti yleisillä ja kaupallisesti saatavilla olevilla tietojenkäsittelykomponenteilla. Virtualisoituja verkkotoimintoja voivat olla esimerkiksi liikennekuorman tasaaminen, palomuurit ja tunkeutumisen havaitsemisjärjestelmät (*Intrusion Detection/Prevention System,* IDS/IPS). Virtualisoidut verkkotoiminnot arkkitehtuuriratkaisuna eivät ole riippuvaisia ohjelmisto-ohjatusta tietoverkosta, vaan niitä voidaan toteuttaa itsenäisesti jo nykyisiä verkko- ja hallintaperiaatteita hyödyntäen. Ohjelmisto-ohjaus (SDN) yhdessä verkkovirtualisoinnin (NFV) kanssa helpottaa verkkojen dynaamista resurssien hallintaa sekä palvelujen ohjausta. Näiden molempien lähestymistapojen yhdistelmällä voidaankin saavuttaa etuja hallinnan ja operoinnin suhteen. [16, kpl 4.4]

Ahmad [2] on väitöskirjassaan listannut edellä SDN:ää vastaan kohdistuviin uhkiin mahdollisia tietoturvaratkaisuja ohjelmisto-ohjatussa tietoverkkoarkkitehtuureissa, jotka on koottu taulukkoon 4.

Tietoturvaratkaisu	Kohdistunut uhka	Ratkaisun kuvaus
Verkkosovellustaso		
FRESCO	Sovellusten uhat	Turvallisuussovellusten kehityskehys
PermOF	Pääsynhallinta	Sovellusten pääsynhallintajärjestelmä
Assertion	Vuosääntöjen ristiriita	Sovellusten virheenkorjauskehys
Flover	Suojauskäytäntöjen rikkomus	Suojauskäytäntöjen varmennussovellus
OFTesting	Vialliset OF-sovellukset	Sovellustestauskehys
Hallintataso		
SE-Floodlight	Sovellusten valtuudet	Suojattu ohjaimen arkkitehtuuri ja turvallinen App-Ctrl-sovellusliittymä
Hybrid Ctrl	Ohjaimen skaalautuvuus	Hybridi (reaktiivinen / proaktiivinen) ohjainarkkitehtuuri
DISCO	Ohjaimen skaalautuvuus	Hajautettu ohjainarkkitehtuuri
Ctrl-Placement & Hyper-Flow	Ohjaimen saatavuus	Kehys ohjaimen sijoittamisesta
DoSDetection	Palvelunestohyökkäykset	Palvelunestohyökkäyksen tunnistamiskehys
Verkkoelementtitaso		
FortNOX	Vuosääntöjen ristiriitaisuus	Ohjainkehys
FlowChecker	Vialliset vuosäännöt	Konfiguraation varmennustyökalu
VeriFlow	Vialliset vuosäännöt	Verkon virheenkorjaustyökalu
Resonance	Pääsynhallinta	Kehys pääsynhallinnan ja käytänteiden täytäntöön panemiseksi.
CPRecovery	Ohjaimen saatavuus	Ohjaimen kopiointijärjestelmä

Taulukko 4. Ohjelmisto-ohjatun tietoturva-arkkitehtuurin tietoturvaratkaisuja [2]

SDN:n verkon keskitetty äly sekä verkon ohjelmoitavuus helpottavat tietoturvauhkien nopeaa tunnistamista ja korjaamista. SDN-verkon näkyvyys ja ohjaus tukevat reaaliaikaista tietoturvan seurantaa sekä verkkolaitteiden tiedonkeruusykleillä keräämää ohjelmointirajapintojen (API) avulla tuotettua analysoitua dataa. Toisin kuin perinteisissä verkoissa, jotka vaativat verkon ulkokehän kalliita tietoturvajärjestelmiä, SDN mahdollistaa johdonmukaisen verkonlaajuisen tietoturvallisuuden täytäntöönpanon sekä ohjelmistomääriteltyjen tietoturvaratkaisujen innovoinnin luoden uudenlaisia tietoturvaratkaisuja. Tästä esimerkkinä *FLOWGUARD* on kattava OpenFlow-verkkojen ohjelmistopalomuurikehys, joka varmistaa palomuurikäytänteiden yhdenmukaisen toteuttamisen koko verkossa. [2, s. 38]

OpenFlow SDN-arkkitehtuuri tarjoaa ohjauksen verkkolaitteille keskitetystä ohjauspisteestä, johon tietoturvapalvelujen lisääminen on yksinkertaista. Tietoturvasovellukset voivat esimerkiksi pyytää pakettinäytteitä ohjaimen kautta käyttämällä yksinkertaisia näytteenottomenetelmiä, kuten FleXam-menetelmää, joka lähettää paketit kokonaisuudessaan tai osan niistä ohjaukseen kytkimen laskuriarvojen perusteella. Sovellus voi suorittaa analyysin ja sitten ohjaimen kautta muuttaa vuosääntöjä, kuten pudottaa peräkkäisiä paketteja tietyistä tietovuoista sovelluksen tietoturvallisuusanalyysiin perustuvien epäilyjen vuoksi. Siksi SDN-konseptista on useita ehdotuksia tietoliikenneverkkojen tietoturvallisuuden suojaamiseksi. [2, s. 39]

Sovellusten tietoturvaratkaisujen suhteen mekanismit, jotka autentikoivat ja valtuuttavat sovellukset ja tarkistavat tällaisten sovellusten luomat vuosäännöt, ovat erittäin tärkeitä. OperationCheckpoint ja PermOF ovat järjestelmiä, jotka myöntävät käyttöoikeudet sovelluksille ja asettavat rajoituksia sovellusten toiminnalle. Ehdotetut mekanismit antavat luvan tiettyihin toimiin liittyville sovelluksille ja voivat siten estää luvattomia muutoksia vuosääntöihin. Yksi OperationCheckpointissa ehdotetun järjestelmän tärkeimmistä eduista on northbound-API -rajapinnan turvaaminen, rajaten siten sovellukset toimimaan vain määritellyllä käyttövaltuusalueella. Suojaussovellusten kehittämistä varten FRESCO tarjoaa puitteet OpenFlow-tietoturvasovellusten nopeaa kehittämistä ja käyttöönottoa varten. [2, s. 39]

Koska ohjaimella on tärkeä rooli SDN-verkoissa, on monia ehdotuksia ja ratkaisuja, jotka vahvistavat itse ohjaimen turvallisuutta. SDN-ohjaimen suojaus on hyvin monitahoinen, koska se vaatii tietoturvaratkaisuja molemmille rajapinnoille kyllästymishyökkäysten vaikutusten lieventämiseksi sekä palvelunestohyökkäysten torjumiseksi. Lisäksi on huomioitava luotettava ohjaimen sijoittaminen. Suojattu (SE, *security enhanced*) Floodlight-ohjain on suojattu versio OpenFlow-floodlight ohjaimesta. SE Floodlight -ohjain turvaa northbound API-rajapinnan, todentaa ja valtuuttaa sovellukset sekä tarkistaa vuosäännöt. On myös northbound API -rajapintaspesifejä tietoturvaratkaisuja, kuten OperationCheckpoint, ja mekanismeja luottamuksen arvioinnin lisäämiseksi ohjaimien ja sovellusten välillä. FortNOX parantaa NOX-ohjainta välttääkseen ristiriitoja sovellusten tuottamissa vuosäännöissä. [2, s. 39-40]

Yhden vikaantumispisteen ongelman välttämiseksi on ehdotettu hajautettuja, mutta loogisesti keskitettyjä ohjaimia. Esimerkiksi HyperFlow on ehdotus skaalattavasta tapahtumapohjaisesta moniohjain-arkkitehtuurista. Useat hajautetut ohjaimet, jotka ovat loogisesti keskitettyjä, tekevät paikallisia päätöksiä vuosääntöjen viiveen minimoimiseksi. Skaalautuvuuden parantaminen lisäämällä ohjainten prosessointikykyä on toinen tapa välttää kylläisyyshyökkäyksiä. Välttääkseen ohjaimen maalittamisen kyllästymishyökkäykselle tai palvelunestohyökkäykselle AVANT-GUARD siirtää yhteystason verkkoelementtitasolle epäonnistuneiden TCP-istuntojen poistamiseksi ja vähentää siten verkkoelementtitason ja hallintatason vuorovaikutuksen määrää. Luotettavaksi ohjaimen sijoittamiseksi ei ole olemassa yhtä oikeaa tapaa, vaan se on kompromissi haluttujen tavoitteiden (kuten redundanssi ja luotettavuus sekä luotettavuus ja viive) välillä. [2, s. 39-40]

Verkkoelementtitason tietoturvaratkaisut vaihtelevat rajapintojen ja vuotaulukoiden turvallisuudesta verkon suunnitteluun ja segmentointiin. Suojausehdotusten, kuten TLS- ja DTLS-salauksen, standardointi on potentiaalinen ratkaisu rajapinnan tai linkkikerroksen tietoturvaan. Oikein konfiguroituna TLS voi tarjota yksityisyyden ja tiedon eheyden kahden osapuolen, kuten ohjaimen ja tiedonsiirtoelementtien, välillä. Lisäksi salausteknisillä suojausprotokollilla, kuten Host Identity Protocol (HIP) -pohjaisilla ratkaisuilla, voidaan varmistaa sekä hyötykuorma että hallita tietoturvaa. [2, s. 40] Namalin et al. [29] artikkelissa on kuvattu tietoturvakehys kontrollikanavalle SDN-ohjauksen ja datatasojen välillä. Artikkelissa ehdotetaan ohjauskanavalle Host Identity Protocol -protokollan käyttämistä TLS (Protocol Layer Security) -protokollan sijasta ratkaisuna ohjauskanavan turvallisuuden sekä SDN:n OpenFlow-arkkitehtuurin liikkuvuuden parantamiseksi.

Vuosääntöjä luovien sovellusten todennus- ja valtuutusmekanismien lisäksi vuotaulukoiden turvallisuus voidaan varmistaa vuosääntöjen varmennusmekanismeilla. Oikea verkon suunnittelu ja segmentointi ovat välttämättömiä toimenpiteitä hallintatason ylikuormittumisen välttämiseksi. Kuormittuminen voi aiheuttaa ohjaimen kyllästymisen, jolloin verkkoelementtitaso ei reagoi verkkoliikenteeseen ja saapuviin tietovoihin. Datatason reitityksen ehjänä pitämiseen tarvitaan verkon sietoisuutta parantavia mekanismeja, jotka mahdollistavat verkon toiminnan häiriötilanteissa, ohjain-kytkin linkin vikaantuessa tai korvattaessa vikaantunut ohjain häiriöttömällä ohjaimella [2, s. 40]

3.3. Kontrolliliikenteen haavoittuvuudet

Kontrolliliikenne on yksi nykyaikaisten viestintäjärjestelmien tärkeimmistä ominaisuuksista, joiden on kyettävä selviytymään spektrin ja ympäristön dynaamisista muutoksista. Kognitiivisten radioverkkojen ollessa kyseessä, on olemassa useita kokonaisuuksia, joiden on vaihdettava kontrolliliikennettä. Yksi niistä on verkonmuodostuminen, joka päivittää säännöllisesti topologiatietoja multi-hop-reititystietojen saamiseksi ja ylläpitämiseksi. Ad hoc -verkot lähettävät lisäksi ”hello”-sanomia salliakseen solmujen liittyä verkkoon ja tarkistaakseen onko hiljainen solmu edelleen kuuluvuusalueella. Taajuuksien havainnointitulokset tulee myös synkronoida yhteisten kanavien tunnistamiseksi. Lisäksi tarvittavista kanavamuutoksista on neuvoteltava. Edellä mainittujen kontrolliliikennettä vaativien kokonaisuuksien lisäksi kognitiiviset toiminteet eivät todennäköisesti rajoitu vain kanavan hallintaan. [1, kpl 4, s. 40]

Myös solmujen luottamuksen hallinta vaatii kontrolliliikennettä epäluotettavien solmujen tunnistamiseksi. Kognitiivisen tietoliikennejärjestelmän luottamuksen hallintaa on käsitelty tarkemmin kappaleessa 3.6. Kontrollikanavalla käydään myös neuvottelua siitä, välittääkö solmu viestit oikein ja voidaanko siihen sen vuoksi luottaa. Kognitiivisen radioverkon on järjestettävä kaikkien näiden tekniikoiden kontrolliliikenne optimaalisella ja turvallisella tavalla keskittyen päästä-päähän ketjun optimointiin. Tämä saattaa edellyttää jopa ylimääräisiä kontrolliresursseja, mikä ei saisi heikentää kuitenkaan käyttäjien tietoliikennettä. [1, kpl 4, s. 40]

Lon mukaan kontrollikanavien suunnittelulle on tunnistettavissa neljä haastetta. Ensimmäinen haaste on välttää kontrollikanavan tukkeutuminen, toinen on häiriösietoisuus, kolmas on peittoalue ja neljäs on tietoturvallisuus. Viides haaste kognitiiviselle radioverkolle on luonnollisesti päästä päähän -suorituskyky. [30]

3.4.1 Kontrollikanavan tukkeutuminen

Kognitiivisen radioverkon kontrollikanavan läpi on kuljettava erilaisia viestejä. Kontrollikanavilla liikennemäärä on todennäköisesti huomattava, riippuen valituista algoritmeista. Kontrollikanavalla välitetään vähintään seuraavia viestejä: [1, kpl 4, s. 42]

- hello-viestit muiden solmujen löytämiseksi ja yhteyksien ylläpitämiseksi
- topologian kontrolliviestit verkon topologian määrittämiseksi ja ylläpitämiseksi
- reititysviestit reittien määrittämistä ja ylläpitämistä varten
- tunnistetut tiedonvaihtoviestit tunnistustietojen jakamiseksi

- kanavanvaihtoviestit kanavanvaihdon aloittamiseksi
- luottamuksenhallinnan tiedonvaihtoviestit
- kerätyt tiedonvaihtoviestit koko järjestelmän oppimisprosessia varten

Edellä mainitut viestit voivat olla joko proaktiivisia tai reaktiivisia, mikä tarkoittaa, että ne ovat joko itse generoituja (esimerkiksi säännöllisesti lähetetyt hello-viestit) tai reagoivat vain muihin tapahtumiin (esimerkiksi kanavanvaihtoviestit reagoivat spektrin käyttöasteen muutoksiin). Kaikkien viestien lähettämisen on tapahduttava tarvittaessa samanaikaisesti ja ne on varustettava eri prioriteeteilla verkon kaikissa solmuissa. On varmistuttava, että kaikki viestit voidaan toimittaa ajoissa, mistä syystä kontrollikanavalla on oltava riittävät resurssit liikenteen tukkeutumisen välttämiseksi. Toisaalta mitä enemmän resursseja on ohjattu kontrollitietojen lähettämiseen, sitä vähemmän resursseja on jäljellä käyttäjien hyötydatan lähettämiseen. Siksi resurssit ovat aina kompromisseja. [1, kpl 4, s. 42]

3.4.2 Häiriösietoisuus

Kontrollikanavat voivat olla joko kaistan sisällä tai kaistan ulkopuolella. Jos kontrolliliikenteelle on varattu kaistan ulkopuolinen ohjauskanava, kognitiivinen radioverkko voi olla pääkäyttäjä (PU = primary user) tällä kanavalla. Siviilimaailmassa tämä on lupaavin tapa välttää häiriöitä muiden käyttäjien kanssa, mutta sotilaallisessa kontekstissa erillinen kontrollikanava muodostaa yhden pisteen vikaantumisen (SPoF), joka on alttiina vihamielisen hyökkääjän häirinnälle. Lisäksi kaistan ulkopuolisen kontrollikanavan tekninen toteuttaminen vaatii joko radioetupään (*RHU*, *radio head unit*) erityisen nopean taajuudenvaihdon tai vaihtoehtoisesti tarvitaan enemmän kuin yksi radioetupää, mikä voi johtaa yhteisvaikutuksiin. Häiriöresistanssi voidaan saavuttaa myös käyttämällä UWB-signaaleja (*ultra wideband*) tai taajuushyppelyä. Jälkimmäinen voi olla myös lähestymistapa häiriöisietoisuuteen kaistan sisäisillä kontrollikanavilla. [1, kpl 4, s. 42]

Mikäli käytetään kaistan sisäistä tai varaamatonta kaistan ulkopuolista kontrollikanavaa ilman taajuushypintää, kognitiivisen radioverkon on reagoitava ilmaantuvaan häiriösignaaliin muuttamalla taajuutta heti, kun häiriö havaitaan. Tämä vaatii kyvyn aloittaa kanavanvaihto signaalin läsnäolosta huolimatta. Kanavanvaihtosanoma on joko lähetettävä eri kanavalla, joka vaatii toisen radion radiopään, tai signaalilla on oltava vastaavuussuhteeltaan riittävän hyvät ominaisuudet, jotta mahdollisesti häirinnän alla oleva vastaanotin havaitsisi sen. [1, kpl 4, s. 42]

3.4.3 Peittoalue

Kaikkien verkon solmujen ei tarvitse käyttää samaa kontrollikanavaa koko ajan, esimerkiksi klusteroinnin avulla verkko voidaan jakaa useisiin aliverkkoihin käyttämällä erilaisia kontrollikanavia. Vaatimuksena on kuitenkin, että kaikkien solmujen välillä on oltava mahdollista vaihtaa kontrollitietoja. Kuten edellä on käsitelty, kontrollikanava voi olla melko staattinen ja siten tarjota ennalta suunnitellun kattavuuden kaikille solmuille, tai se voi olla dynaaminen ja yhdistää vain muutaman solmun pyynnöstä. Vaikka staattinen kontrollikanava on altis häiriöille, dynaaminen ohjauskanava vaatii enemmän resursseja yhteyksien muodostamiseksi. Erityisesti liikkuvissa Ad Hoc -verkoissa on otettava huomioon kontrollikanavan taajuusalue. [1, kpl 4, s. 43] Esimerkiksi UWB-signaaleilla on hyvin pieni kantama, ja siksi niitä voidaan käyttää vain verkoissa, joissa solmujen enimmäisetäisyys seuraavaan naapuriinsa on enintään 100 metriä [31].

3.4.4 Tietoturvallisuus ja tiedon eheys

Kuten edellä on jo mainittu, kontrollikanavat muodostavat yhden pisteen vikaantumisen mahdollisuuden, koska kognitiivisen radioverkon solmut eivät kykene kommunikoimaan ilman toimivaa kontrolliliikennettä. Siksi kontrolliliikenteen luottamuksellisuus, eheys ja saatavuus ovat tärkeitä kysymyksiä kognitiiviselle radioverkolle. On varmistettava, että naapureiden kontrollitiedot eivät ole vääriä tai viallisia. [1, kpl 4, s. 43]

3.4.5 Päästä-päähän suorituskyky

Kognitiivisen radioverkon kontrollisanomilla tulee olla erilaiset prioriteetit. Jotkin viestit, kuten taajuuden muutosviestit, on lähetettävä erittäin nopeasti. Siksi verkolla on oltava hyvä päästä-päähän suorituskyky hyvin pienellä viiveellä. Yksi viivettä aiheuttava tekijä on viestien edelleen lähettäminen usean hypyn yli, mikäli viestin lopullinen vastaanottaja on alkuperäisen lähettimen peittoalueen ulkopuolella. Mitä vähemmän solmuja on suorassa yhteydessä toisiinsa, sitä enemmän viestejä on välitettävä edelleen, mikä kuluttaa edelleen lähettävien solmujen resursseja ja lisää viivettä. Klusteroiduissa verkoissa klusterien välinen viestintä johtaa edelleen lisääntyneeseen viiveeseen, koska viestin välittävien yhdyskäytäväsolmujen on vaihdettava lähetystaajuutta. Sotilaallisessa kontekstissa viiveen lisäksi viestien priorisointi on tärkeää suorituskyvyn kannalta. Siinä on huomioitava myös sotilaalliset johtosuhteet ja joukkorakenteet. Lisäksi on suunniteltava mitä ryhmäviestijärjestelmiä tarvitaan (unicast, broadcast, multicast). [1, kpl 4, s. 43]

3.4. Kontrolliliikenteen toimintavarmuutta parantavat vaihtoehdot

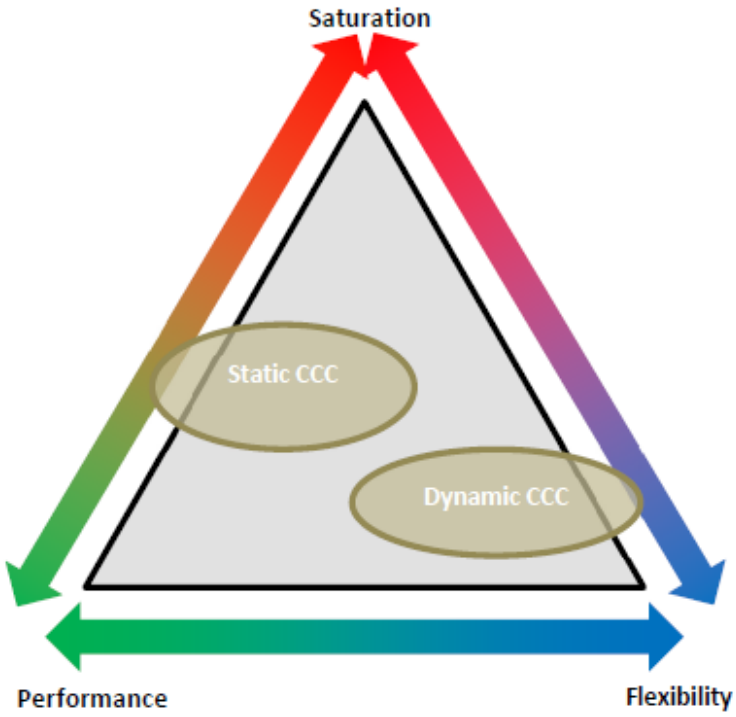
Jotta kirjallisuudessa ehdotettuja kontrollikanavien suunnittelumalleja voidaan vertailla, on niitä luokiteltu seuraavien ominaisuuksien mukaan: järjestelmätyyppi (sekvenssipohjainen, ryhmäpohjainen, dedikoitu tai UWB), allokointi (kaistan sisäinen, kaistan ulkopuolinen) ja kattavuus (käytetäänkö kontrollikanavaa muodostamalla solmuista aliverkkoja vai globaalisti kaikissa solmuissa). Lisäksi verrataan radioissa tarvittavien lähetin-vastaanottimien lukumäärää samoin kuin sitä, vaatiiko kontrollikanavasuunnittelu solmujen synkronointia ja mekanismeja naapurin löytämiseen. Edellä mainituilla mittareilla voidaan osoittaa, vastaavatko ehdotetut järjestelmäsuunnitelmat kontrollikanavan tukkeutumisen, ensisijaisen käyttäjän aktiivisuuden robustisuuden, peittoalueen ja kontrollikanavan häirinnän haasteisiin. [1, kpl 4, s. 41]

Kontrollikanavan suunnittelulle on periaatteessa kaksi lähestymistapaa. Aluskerros-malli (*underlay*) voidaan toteuttaa esimerkiksi UWB-signaaleilla. Tämä toteutus on robusti, mutta se mahdollistaa vain lyhyet etäisyydet solmujen välillä. Siksi aluskerros-mallia voidaan suositella vain melko staattiselle verkon kokoonpanolle lyhyillä välimatkoilla, esimerkiksi tukikohdassa käytettäväksi. Liikkuvissa sovelluksissa vaaditaan päällyskerroksen (*overlay*) kontrollikanavia. Kontrollikanavan peiton suhteen solmuilla voi olla suuri etäisyys toisistaan, mutta ne ovat alttiimpia häiriöille. Koska kontrollikanavat muodostavat yhden pisteen vikaantumisen mahdollisuuden, on ne suunniteltava huolellisesti. Kiinteän fyysisen kanavan käyttämistä ei suositella, koska se on helposti häirittävissä. Toisaalta puhtaasti mukautuvat kontrollikanavat, jotka voivat dynaamisesti väistää häirityt taajuuskaistat, haittaavat naapuruuksien muodostumista. [1, kpl 4, s. 44]

Yhden pisteen vikaantumisen välttäminen kontrolliliikenteessä on ensiarvoisen tärkeää kognitiiviselle radioverkolle. Mahdollisia ehdotettuja ratkaisuja tähän ovat hajaspektritekniikat, dynaaminen kontrollikanavan allokointi ja häiriösietoisten avainten jakelutekniikoiden käyttö haavoittuvan tiedon (esim. sijainnin) suojaamiseksi. [1, kpl 4, s. 44-46] Taajuushyppelyaaltomuodot ovat vaikeammin häirittävissä kuin kiinteiden taajuuksien aaltomuodot. Hajaspektritekniikat ovat olleet jo pitkään käytössä sotilaallisissa johtamisjärjestelmissä. Niiden käyttö on ollut yleinen toimenpide häirinnän väistämiseksi, mutta niistäkin tulee tehottomia, mikäli vastustaja saa tietoonsa käytetyt hyppyparametrit. Lisäksi hyppykuvion on otettava huomioon kanavien heterogeeninen saatavuus [1, kpl 4, s. 44-46]. Koslowski et al. ovat artikkelissaan esittäneet esimerkin adaptiiviselle taajuushyppelyalgoritmille [32]. Hajaspektritekniikat ovat myös aina kompromissi tarvittavan tiedonsiirtokapasiteetin ja häirinnänsiedon välillä.

Kysymys siitä, onko staattinen tai dynaaminen kontrollikanava suotuisa, riippuu ohjausliikenteen määrästä ja lähetystiheydestä. Staattinen kontrollikanava edellyttää, että kaikki laitteet käyttävät samoja hyppyparametrejä, kun taas dynaaminen kontrollikanava vaatii vain, että käytetyt taajuudet tunnetaan. Dynaamisessa kontrollikanavassa solmu tarkkailee yhtä tai useampaa näistä taajuuksista, mikä voi viedä useita aikavälejä (*time slot*), kunnes lähetin ja vastaanotin ovat löytäneet toisensa. Infrastruktuuriverkossa, joka on melko staattinen eikä siksi vaadi juurikaan päivityksiä topologiaan ja taajuus-saatavuuteen, dynaaminen kontrollikanava voi olla riittävä. Mikäli on olemassa uhka vihollisen ELSO:sta, voi olla, ettei liikkuvan verkon dynaamisesti muodostuvalla kontrollikanavalla ole tarpeeksi aikaa neuvotella kontrollikanavan muodostumiseksi. Tästä syystä staattinen kontrollikanava voi osoittautua toteuttamiskelpoisemmaksi ratkaisuksi. [1, kpl 4, s. 44]

Kuten kuva 11 osoittaa, staattisen tai dynaamisen kontrollikanavan välillä tehtävä päätös on kompromissi suorituskyvyn, joustavuuden ja kontrolliliikenteen tukkeutumisen suhteen. Vaikka dynaaminen kontrollikanava voi joustavasti mukautua tiedonvaihtotarpeisiin ja välttää siten liikenteen kyllästymisen, neuvottelut kontrollikanavan muodostamisesta heikentävät kokonaissuorituskykyä. Puhtaasti staattiset kontrollikanavat eivät tarvitse tällaisia neuvotteluja, mutta toisaalta eivät voi myöskään sopeutua vaihtelevaan kontrollitietojen vaihtoon. [1, kpl 4, s. 45]



Kuva 11. Kontrollikanavien ominaisuudet suhteessa verkon suorituskykyyn, joustavuuteen ja kyllästymiseen [1, kpl 4, s. 45]

Kontrollikanavan tukkeutumisen välttämiseksi sille on osoitettava riittävä kaistaleveys. Mirhoseninejad et al. [33] ovat kuvanneet konferenssijulkaisussaan mahdollisen tekniikan jakaa kontrollikanava useisiin alikanaviin, jotka voidaan dynaamisesti allokoida lähetystä varten. Yleensä muuttuva kaistanleveys sallii dynaamisen kompromissin kontrolliliikenteen ja hyötylähetteen välillä, mutta muodostaa haasteen topologian muodostamiselle. Ympäristöstä riippuen voi olla kanavia, joilla on erilainen kaistaleveys, linkin laatu tai yhdistelmä muita naapurikanavia. [1, kpl 4, s. 45]

Häiriösietoisuuden suhteen häirintäsignaali vaatii verkolta asianmukaisen reaktion. Tämän reaktion on oltava yhteinen kaikille vaikutuksen alla oleville solmuille, mikä tarkoittaa, että ne esimerkiksi aloittavat väistötoimet uudelle kanavalle samanaikaisesti. Häirinnän takia ei yleensä ole mahdollista neuvotella uutta yhteistä kontrollikanavataajuutta, mistä johtuen on tärkeä ennalta suunnitella häirinnän väistöparametrit ja reaktiot. Luonnollisesti tämä vaatii nopeamman häirinnänväistöreaktion, kuin mihin häirintälähetin kykenee. [1, kpl 4, s. 45]

Yksi ratkaisu häirinnän väistöprosessiin on sellaisten signaalien lähettäminen, joilla on hyvät korrelaatio-ominaisuudet. Käytettäessä CDMA-koodijakokanavointia ennalta määriteltyjen jakokoodien kanssa erilaisten ilmoitusten vastaanottaminen on mahdollista. Mikäli käytettävissä on kaksi radioetupäätä, häirityn kanavan väistöstä voidaan antaa ilmoitus toisen radioetupään kautta vapaalla kanavalla. Samankaltainen ehdotus on esitetty Rauschenin et al. [34] konferenssijulkaisussa, mutta tässä ehdotuksessa on käytetty vain yhtä laajakaistavastaanottimella varustettua radioetupäätä. Tämä laajakaistavastaanotin jakaa spektrin pienemmiksi kanaviksi ohjelmiston avulla, välttäen siten kahden radioetupään yhteiskäyttövaikutukset. Siitä huolimatta käytettyjen kanavien välistä taajuusväliä rajoittavat vastaanottimen ominaisuudet, esimerkiksi kaistanleveys ja laitteistosuodattimet. [1, kpl 4, s. 46]

Päästä-päähän suorituskyvyn optimointi on yksi tärkein kognitiivisen radioveron tehtävistä. Päästä-päähän suorituskyvyn suhteen staattinen kontrollikanava on nopeampi kuin dynaaminen, koska käytettyä taajuuskaistaa ei tarvitse neuvotella tai tunnistaa. Myös klusteroinnilla on suuri vaikutus kokonaissuorituskykyyn, koska taajuuden muutokset klusterin rajapinnoilla lisäävät viivettä. Ratkaisu tähän voi olla kahden radioetupään käyttö (kommunikointiin kahdella taajuudella samanaikaisesti, ellei toista tarvita kanavan häirinnän väistöön, kuten aiemmin on esitetty) tai suurempien klusterien muodostaminen. Suuremmat klusterit merkitsevät vähemmän aliverkkoja ja siten vähemmän rajapintoja, mutta toisaalta ne vaativat enemmän lähetystehoa. Lisäksi suuret klusterit, joissa on enemmän laitteita, tarvitsevat pienempiä klustereita enemmän kontrolliliikennettä klusterin sisäiseen organisointiin, mikä on otettava huomioon tarkasteltaessa kontrollikanavan tukkeutumista. [1, kpl 4, s. 46]

Kontrollisanoman viive alentaa järjestelmän päästä päähän -suorituskykyä. Tämän viiveen aiheuttama vaikutus voi vaihdella viestin tyypistä riippuen. Esimerkiksi myöhästyneet topologian ohjaussanomat tai reititysviestit voivat johtaa merkittävään viiveeseen tai virheellisesti reititettyjen viestien menetykseen. Viivästyneillä hello-viesteillä ei pitäisi olla suoraa vaikutusta, mutta solmun verkosta poissulkemiseen johtavaa useampien hello-viestien puuttumista on vältettävä. Taajuushavainnointiin liittyvien viestien myöhästyminen voi johtaa vääriin kanavanvaihtopäätöksiin. Erityisen kriittisiä ovat myöhästyneet kanavanvaihtoviestit, koska ne voivat johtaa solmujen sulkeutumiseen ulos verkosta. Viestien viiveen vaikutusten minimoimiseksi viestityyppien priorisointi on tärkeää. [1, kpl 4, s. 46-47]

Kontrolliliikenteen eheys on myös erityisen tärkeää. Väärennetty tai viallinen kontrolliliikenne voi saada verkon toimimaan ei halutulla tavalla. Kontrolliliikenteen luottamuksellisuus voidaan tarkistaa luottamuksenhallinnan avulla. Luottamuksenhallinnan viivästynyt tietojenvaihto voi johtaa vääriin luotettavuuspäätöksiin (luottamuksenhallintaa on käsitelty tarkemmin kappaleessa 3.6). [1, kpl 4, s. 46-47]

3.5. Taajuushavainnointiin kohdistuvat hyökkäykset

Taajuushavainnointi (SS, *spectrum sensing*) on yksi kognitiivisen radion olennaisimmista mekanismeista ja yksi hyvin aktiivisista tutkimusalueista. Vaikka taajuushavainnoinnin toiminnallisia näkökohtia on tutkittu aktiivisesti, sen turvallisuusnäkökohdat ovat saaneet hyvin vähän huomiota. Kuten muutkin verkot, myös kognitiiviset radioverkot ovat alttiina useille turvallisuusuhkille. Kognitiivisen radioverkon yhteistyömalli itsessään aiheuttaa erilaisia turvallisuusuhkia. Taajuushavainnointia kohtaan kohdistuvista hyökkäyksistä on määritelty kaksi hyökkäystapaa: 1) ensisijaisen käyttäjän emulointihyökkäys (IE, *incumbent emulation*) ja 2) taajuushavainnoinnin väärentämishyökkäys (SSDF, *spectrum sensing data falsification*), jota myös kutsutaan Bysanttilaishyökkäykseksi (*Byzantine* attack). [10; 14; 22]

Ensisijaisen käyttäjän emulointihyökkäyksissä, eli IE-hyökkäyksissä jotkut verkon kognitiivisista radioista tai verkon ulkopuoliset toimijat yrittävät jäljitellä ensisijaisen käyttäjän lähetystä häiritäkseen taajuudenhavainnointia. IE-hyökkääjien läsnäolo saa kognitiivisen radioverkon fuusiokeskuksen päättämään, että tarkasteltavana oleva taajuuskaista ei ole käytettävissä. [14] Käytännössä tämä johtuu kognitiivisen radioverkon toimintaperiaatteesta, jossa havaitessa ensisijainen käyttäjä tietyllä kaistalla, kaikki toisiokäyttäjät välttävät tämän kaistan käyttöä. Kun toisiokäyttäjä havaitaan, muut toisiokäyttäjät voivat halutessaan jakaa saman kaistan. Toisin sanoen ensisijaisilla käyttäjillä on taajuusresursseihin pääsyssä korkeampi prioriteetti kuin toisiokäyttäjillä. IE-hyökkäyksessä pahantahtoinen toisiokäyttäjä yrittää saavuttaa etusijan muihin toissijaisiin käyttäjiin nähden lähettämällä signaaleja, jotka jäljittelevät ensisijaisen käyttäjän ominaisuuksia. [10]

Kognitiivisten radioiden ohjelmoitavuudesta johtuen vastustajan on mahdollista muokata kognitiivisen radion ohjelmistoa sen lähetysparametrien (esimerkiksi moduloinnin, taajuuden ja tehon) suhteen siten, että lähetteen tunnuspiirteet muistuttavat ensisijaisen käyttäjän ominaisuuksia. IE-hyökkäyksen potentiaaliset vaikutukset riippuvat aitojen toisiokäyttäjien kyvystä erottaa hyökkääjän signaali todellisista ensisijaisen käyttäjän signaaleista suorittaessaan taajuushavainnointia. [10] Alla on käsitelty kahta olemassa olevaa taajuushavainnointitekniikkaa ja selvitetty, miksi ne voivat olla alttiita IE-hyökkäyksille.

Vastaanotetun tehon havainnointi on yksinkertaisimpia menetelmiä taajuushavainnoinnissa. Energianilmaisin päättelee ensisijaisen käyttäjän olemassaolon mitatun signaalienergiatason perusteella. Selvästikään vastaanottotehon mittaamisen avulla ei pystytä erottamaan ensisijaisen ja toisiokäyttäjän signaaleja toisistaan. Tästä syystä on ehdotettu paranneltua mittausjärjestelmää, joka hyödyntää määräajoin suoritettua hiljaisten jaksojen käyttöä. Helpottaakseen taajuushavainnointia hiljaisen jakson aikana mikään toisiokäyttäjä ei lähetä signaaleja. Kun kaikki toisiokäyttäjät havaitsevat hiljaisia jaksoja, ensisijaisten käyttäjien havaitseminen tulee suoraviivaiseksi. Toisin sanoen mitä tahansa lähetettä, jonka vastaanotetun signaalin energiataso ylittää tietyn kynnyksen, voidaan pitää ensisijaisena käyttäjänä. Tällainen havaitsemisstrategia ei kuitenkaan toimi silloin, kun haitalliset toisiokäyttäjät lähettävät tarkoituksella hiljaisina aikoina. Signaalien ominaisuuksien havainnointi on vaihtoehtoinen tekniikka, joka käyttää joko syklostationaarisen ominaisuuden ilmaisua tai suodatintunnistusta ensisijaisen käyttäjän signaalin parametrien tunnistamiseksi. Pelkästään signaalitoimintojen tunnistukseen luottaminen ei kuitenkaan välttämättä riitä erottamaan ensisijaisen käyttäjän signaalia hyökkääjän signaalista. [10]

Vastustajalla voi olla kaksi erilaista motiivia IE-hyökkäysten käynnistämiseksi. Koska toisiokäyttäjät välttävät sellaisen taajuusalueen käyttöä, missä havaitaan ensisijaisen käyttäjän signaali, hyökkääjä voi estää ja monopolisoida vapaan kaistan, mikäli se onnistuu uskottelemaan olevansa ensisijainen käyttäjä. Tällaista hyökkäystä kutsutaan itsekkääksi IE-hyökkäykseksi. Toinen motiivi on estää aitojen toisiokäyttäjien pääsy taajuusalueille aiheuttaen siten palvelunestohyökkäyksen. Tätä hyökkäystä kutsutaan haitalliseksi IE-hyökkäykseksi. [10]

Chen et al. ovat artikkelissaan [10] toteuttaneet simulaation IE-hyökkäyksestä. Simulaation tulokset osoittavat IE-hyökkäysten tehokkuuden. Simulaatio osoittaa, että molemman tyyppiset IE-hyökkäykset voivat vähentää huomattavasti käytettävissä olevia kaistanleveysmahdollisuuksia, mitä kukin aito toisiokäyttäjä voi havaita. Tulosten mukaan haitalliset IE-hyökkäykset häiritsevät enemmän käytettävissä olevan kaistanleveyden saatavuutta. [10]

Avain IE-hyökkäyksiltä puolustautumiseen on kehittää robusti tekniikka ensisijaisen käyttäjän signaalin aitouden todentamiseksi. Yksi mahdollinen lähestymistapa on käyttää signaalin todentamista fyysisessä kerroksessa käyttämällä RF-signaalin ominaisuuksia, jotka liitetään tietyn lähettimen tai lähettimien ominaisuuksiin, tai yksinkertaisesti lisäämällä varmenteita ensisijaisen käyttäjän signaaliin. Fyysisen kerroksen todennuksella vältetään ylemmän kerroksen todennukseen liittyvät otsikkotiedot, mutta se voi olla vähemmän luotettava, koska ominaisuudet tai varmenteet ovat signaalin heikkenemisen kohteena. Toinen menetelmä on käyttää todennusprotokollaa ensisijaisen käyttäjän lähettimen ja todentajan välillä. [22, s. 14]

Yksi ehdotettu ratkaisu koostuu ennakoivista (pikemminkin kuin reaktiivisista) hyppyparametreista kanavalta kanavalle, tai kanavan hypyn yhdistämisestä muiden toimintojen kanssa. Ennakoidut hyppyparametrit vaikeuttavat kuitenkin hyppyparametrien mallintamista. Ennakoiva taajuushypintä ei ole siitä syystä välttämättä toivottava ratkaisu, koska se lisää verkon dynamiikkaa ja otsikointien ja kontrolliliikenteen määrää, mikä vähentää suorituskykyä muun tietoliikenteen osalta. Ennakoivasta hypytyksestä aiheutuva kompleksisuus asettaa verkkoon lisäkuormitusta vain DSA:n käyttöön liittyvien haavoittuvuuksien vähentämiseksi, mikä olisi otettava huomioon DSA:n käyttöönotossa. [22, s. 14-15]

Mahdollinen ratkaisu on myös kiinteiden ensisijaisten käyttäjien kohdalla hyödyntää paikkatietoa varmennukseen. Ensisijaisilla käyttäjillä on yleensä vahvempi lähetysteho kuin toisiokäyttäjillä. Kun tiedossa on ensisijaisen käyttäjän paikkatieto sekä lähetysteho, voidaan verrata vastaanotetun signaalin tehotasoa laskennalliseen tasoon. Tässä haastavan tehtävän muodostaa signaalin lähteen sijainnin todentaminen. Sijainnin varmennusjärjestelmän on oltava ei-vuorovaikutteinen, mistä johtuen sijainnin todentava laite ei voi olla vuorovaikutuksessa signaalilähettimen kanssa arvioidakseen tai todentaakseen sen sijaintia. [10]

Etäisyyden hyödyntämiseksi ensisijaisen käyttäjän tunnistamisen haasteisiin esitetään kahta tekniikkaa. Ensimmäistä tekniikkaa kutsutaan etäisyyssuhteeksi (DRT, *distance ratio test*), joka käyttää vastaanotetun signaalinvoimakkuuden (RSS, *received signal strength*) mittaustuloksia, jotka on saatu sijaintitodentajilta (LV, *location verifiers*) lähettimen sijainnin varmistamiseksi. Sijaintitodentaja voi olla erillinen verkkolaite tai toisiokäyttäjä, jolla on tehostetut toiminnot paikannustarkistuksen suorittamiseksi. Yksittäiset LV-solmut muodostavat edelleen verkon ja ovat yhteydessä toisiinsa. Niiden tiedonsiirto tulee turvata tietoturvaprotokollalla. Koska langattoman linkin etäisyyden ja RSS:n välillä on vahva korrelaatio, RSS-mittaukset kahdella LV:llä korreloivat niiden vastaaviin etäisyyksiin lähettimen sijainnin suhteen. [10]

RSS-arvo riippuu myös lähettimen ominaisuuksista, kuten lähetystehosta ja antennin vahvistuksesta. Mikäli kaksi LV:tä käyttää identtisiä radiovastaanottimia ja suorittaa synkronoituja mittauksia, voidaan osoittaa, että vapaan tilan etenemismallissa niiden RSS-mittausten välinen suhde riippuu vain vastaanottimen ja lähettimen sijainnin etäisyydestä. Siksi kunkin LV:n ja lähettimen välisten etäisyyksien suhde voidaan laskea käyttämällä kahden LV:n sijaintitietoja ja ensisijaisen lähettimen oletettua sijaintia. Tätä suhdetta verrataan suhteeseen, joka saadaan RSS-mittauksista, jotka on otettu kustakin LV:stä. Jos odotettu arvo ja mitattu arvo ovat riittävän lähellä (ennalta määritetyn tarkkuuden perusteella), lähetin läpäisee sijaintitestin ja se todetaan ensisijaiseksi käyttäjäksi. [10]

DRT-tekniikan toimivuuteen vaikuttaa kuitenkin tosiasiallinen radioaallon eteneminen, mihin puolestaan vaikuttavat erilaiset ympäristömuuttujat. Erilaiset ympäristöt voivat vaatia erilaisten parametrien käyttöä, mikä edellyttää jopa täysin erilaisten etenemismallien käyttöä. Tällaisten ongelmien ratkaisemiseksi tarvitaan tehokkaampia tekniikoita. [10]

Toista tekniikkaa kutsutaan etäisyyserotestiksi (DDT, *distance difference test*). Tämä tekniikka hyödyntää signaalin vaihe-eroa. Kun signaali lähetetään yhdestä lähteestä kahteen LV:iin, voidaan havaita suhteellinen vaihe-ero johtuen niiden välisestä etäisyydestä. Vaihe-ero voidaan taas muuntaa aikaeroksi, joka puolestaan voidaan muuntaa etäisyyseroksi. Täten voidaan laskea kunkin LV:n ja lähettimen oletettujen keskinäisten etäisyyksien ero käyttämällä kahden LV:n sijaintitietoja ja ensisijaisen lähettimen oletettua sijaintia. Tätä oletettua eroa verrataan mitattuun eroon ensisijaisen käyttäjän signaalin aitouden määrittämiseksi. Jos nämä kaksi arvoa ovat riittävän lähellä, lähetintä pidetään ensisijaisena käyttäjänä. Vaikka DDT ei kärsi DRT:n haitoista, DDT vaatii LV:ien välillä tehokasta synkronointia (satojen nanosekuntien luokkaa), jonka toteuttaminen voi olla kallista. [10]

Toinen turvallisuusuhka hajautetulle taajuushavainnoinnille on väärien taajuustunnistustietojen lähettäminen haitallisten toisiokäyttäjien toimesta. Hyökkäystä kutsutaan taajuushavainnoinnin väärentämishyökkäykseksi (SSDF, *spectrum sensing data falsification*). Toinen yleinen nimitys tällaiselle hyökkäykselle on Bysantilaisyökkäys (*Byzantine attack*). SSDF-hyökkäyksessä jotkut kognitiiviset radiot esittävät vääriä taajuushavainnointitietoja häiritäkseen fuusiokeskuksen taajuushavainnointiprosessia. Hyökkääjä voi lähettää virheellisiä paikallisia taajuusmittaustuloksia fuusiokeskukselle, mistä aiheutuu fuusiokeskuksen väärä päätös käytetyistä taajuuksista. Hyökkääjän pyrkimyksenä on hyödyntää fuusiokeskuksen virheellistä päätöksentekoa omien etujen saavuttamiseksi, esimerkiksi lisääntyneellä spektrin saatavuudella tai itselleen saamalla kapasiteetilla. [10; 14; 22, s. 15]

Jotta fuusiokeskuksen päätöksentekokyky kyetään pitämään riittävän tarkkana jopa SSDF-hyökkäysten keskellä, on DSS:ssä käytetyn datafuusiotekniikan oltava riittävän robusti haitallisten toissijaisten käyttäjien ilmoittamien paikallisten taajuushavainnointitulosten virheellisyyden suhteen. Vaikka DSS:lle on hiljattain ehdotettu muutamia datafuusiotekniikoita, mikään ei ole toistaiseksi ratkaissut tätä ongelmaa. Chen et. al [10] ovat esittäneet kolme datafuusiotekniikkaa DSS:n toimintaan liittyen. Kutakin tekniikkaa on kuvailtu lyhyesti ja pohdittu niiden haavoittuvuuksia SSDF-hyökkäyksiin.

Ratkaisuksi SSDF-hyökkäyksiä vastaan on ehdotettu kaksitasoista puolustusta. Ensimmäisellä tasolla kaikkien paikallisten taajuushavainnointitulosten on oltava todennettuja tietojen kerääjän (LV) toimesta. Tämän turvatoimenpiteen tarkoituksena on estää kognitiivisen radioverkon ulkopuolelta tulevat toistohyökkäykset tai väärien tietojen injektiot. Toinen puolustustaso SSDF-hyökkäysten suhteen on riittävän robustin datafuusiotekniikan käyttöönotto. Kuten aiemmin on käsitelty, nykyiset datafuusiotekniikat ovat alttiita SSDF-hyökkäyksille. Niitä voidaan parantaa kahdella tavalla. Yksi tapa on käyttää peräkkäistä todennäköisyyssuhdetestiä (SPRT, *Sequential Probability Ratio Test*), joka on paikallisten taajuuksien mittaustuloksia tukeva datafuusiotekniikka. SPRT:llä on kyky vähentää sekä väärien hälytysten että uhkien havaitsemattomuuden todennäköisyyttä. Vaikka jokaisella anturilla olisi heikko taajuushavainnointitarkkuus, SPRT voi taata hyvän havainnointitarkkuuden keräämällä lukuisia paikallisia taajuushavainnointituloksia. Toinen tapa lisätä datafuusioprosessin vakautta on ottaa maineeseen perustuva turvajärjestelmä käyttöön DSS-prosessissa. [10] Maineeseen perustuvia ratkaisuja on käsitelty tarkemmin kappaleessa 3.6

Yhtenä mahdollisuutena SSDF-hyökkäysten torjumiseksi on ehdotettu myös painotettua peräkkäistä todennäköisyyssuhdetestiä (WSPRT, *weighted sequential probability ratio test*). Tämä lähestymistapa on samankaltainen kuin monet luottamukseen perustuvat tietojen fuusiojärjestelmät. Tapauksissa, joissa SSDF-hyökkäys ei ole kyennyt saamaan fuusiokeskusta täysin kyvyttömäksi toimia, nämä järjestelmät ovat osoittaneet tyydyttävää suorituskykyä. Niiden suorituskykyä ei ole kuitenkaan vielä analyyttisesti tutkittu. Viimeisimmissä tutkimuksissa on pyritty tunnistamaan hyökkäystä toimeenpanevat solmut. Niissä ehdotetaan haitallisten solmujen havaitsemisjärjestelmiä, jotka perustuvat ulkopuolisiin havaitsemistekniikoihin, joissa fuusiokeskuksen oletetaan tietävän paikallisten anturien vastaanottamat tarkat signaali-kohinasuhdearvot. [14]

Myös artikkelissa [14] esitetään luottamuksenhallintajärjestelmää yhtenä mahdollisuutena SSDF-hyökkäysten torjumiseksi. Helppo, tehokas ja nopea maineeseen perustuva havaitsemisjärjestelmä voi tunnistaa bysanttilaiset hyökkääjät laskemalla paikallisten päätösten ja fuusiokeskuksen tekemien globaalien päätösten väliset epäsuhteet tietyllä ajanjaksolla ja poistamalla sitten SSDF-hyökkääjien syöttämän datan fuusioprosessista.

3.6. Luotettavuuden arviointiin perustuvat kognitiivisen tietoliikennejärjestelmän turvallisuutta parantavat toteutusvaihtoehdot

3.6.1. Luotettavuuden arviointi

Muun muassa Mukherjeen ja Nathin [35] mukaan tunkeutujien (haitalliset toisiokäyttäjät) tunnistamiseksi on käytettävä luotettavuuden arviointia kognitiivisissa tietoliikenneverkoissa. Kognitiivisten tietoliikenneverkkojen tunkeutumisen havainnoinnissa tehtävänä on paljastaa toisiokäyttäjät, jotka tuottavat valheellista informaatiota järjestelmään. Tällaista hyökkäystapaa hyödyntävät muun muassa Bysantilaishyökkäys sekä SSDF-hyökkäys. [35] Erityisen monessa lähteessä ehdotetaan luottamuksenhallintajärjestelmää, joka perustuu toisiokäyttäjien ja ensisijaisten käyttäjien välillä tapahtuvan tiedonvaihdon seurantaan mahdollisten tietovääränösten tunnistamiseksi. [1, kpl 4, s. 35].

Järjestelmän kognitiivisten päätösten luottamusaste voidaan arvioida suorien vuorovaikutusten, havaintojen ja suositusten perusteella. Epäluotettavien suositusten löytämiseksi kerätty data voidaan painottaa lähettäjän luottamuskertoimella. Luottamuksen arvioinnissa käytettyjen tietolähteiden erilainen laatu on myös otettava huomioon. Ratkaisuehdotuksena on toiminto, jossa luottamusluokitus muuttuu arviointikriteerien perusteella. Arviointikriteerit jakavat eri painoarvoja erityyppiselle käyttäytymiselle. Solmu määrittää korkeimmat painoarvot sen itsensä tunnistamiin tapahtumiin. Pienemmät painoarvot määritetään tapahtumille, jotka havaitaan solmun läheisyydessä, ja vastaavasti pienimmät painoarvot määritetään lokiraporteista kerätyille tiedoille. Luotettavuuden arviointiin voidaan sisällyttää myös arviointiprosessi, joka viittaa tietoturvasääntöihin, sertifikaattien vaihtoon, ja riskinarviointiin. [1, kpl 4 s. 34]

Kalaiselvan ja Kavitha ehdottavat kognitiiviselle radioverkolle luottamuksen arviointimallia, jossa luottamustaso muihin solmuihin nähden lasketaan perustuen vain solmun suoriin havaintoihin (vain sen solmun generoima signalointi). Muut solmut tunnistavat ja tulkitsevat tämän solmun tuottamaa informaatiota perustuen sen ”maineeseen”. Suorat solmujen havainnot johtavat Bayesin analyysiin, ja mainejärjestelmä perustuu taas Dempster-Shafer-teoriaan. [36] Bayesilaisessa tilastotieteessä ajatellaan, että havainnot tunnetaan jolloin ne ovat kiinteitä, ja itse todellisuus on tuntematon, johon liittyy epävarmuutta. Tarkoituksena on laskea posterioritodennäköisyyksiä siten, että otetaan huomioon sekä ennakkotieto että havaintoaineiston informaatio. [37]

Edellä esiteltyä Dempsterin-Shaferin teoriaa käytetään erityisesti silloin kun lähdetieto on ristiriitaista, epävarmaa tai puutteellista. [1, kpl 4 s. 34-35] Todennäköisyysteorialla voidaan mallintaa epävarmuutta, mutta on olemassa kuitenkin tietoa (kuten tietämättömyys), jota todennäköisyyslaskenta ei pysty kuvaamaan. Dempsterin-Shaferin teorialla voidaan yhdistää uskomusta tukevia todisteita eri lähteistä ja saada tulokseksi määre, jolla mitataan uskomusta tukevan näytön uskottavuuden astetta (*degree of belief*), ja funktio, joka huomioi kaikkien saatavilla olevien todisteiden uskottavuuden (*belief function*). [38]

Luottamuksen arviointiprosessi voi perustua myös useista informaatiolähteistä peräisin olevaan tietoon. Tämä tieto voi olla monimutkaista sekä luotettavuudelta ja laadultaan erilaista. Kaikki tieto olisi yhdistettävä kuitenkin yhtenäiseksi ja tarkaksi kokonaisuudeksi. Tämä edellyttää tarkoitustenmukaisten fuusiotekniikoiden käyttöönottoa, mikä mahdollistaa virheellisten tai epätarkkojen uhkien tunnistamisen. Erilaiset todennäköisyyslaskelmat ovat yleisin käytetty tekniikka kohteen luottamustasotason arviointiin. [1, kpl 4 s. 34]

Todennäköisyyslaskennan lisäksi on myös ehdotettu sumean logiikan (*fuzzy logic*) käyttöä [1, kpl 4 s. 34]. Sumea logiikka on matemaattisen logiikan laajennus, jossa propositiolla on diskreetin totuusarvon (tosi tai epätosi) sijasta reaalinen totuusarvo suljetulla välillä nollasta yhteen. Sumea logiikka korvaa kaksiarvoisen logiikan ja monimutkaiset matemaattiset mallit yksinkertaisilla, ihmisen todellista päättelyä muistuttavilla kielellisillä malleilla. Luotettavuusarvioinnissa totuusarvo voi olla jotakin välillä ”täysin luotettava” ja ”ei lainkaan luotettava”. [39]

Maineeseen perustuvan järjestelmän suunnittelussa voidaan lainata myös ideoita jo olemassa olevasta tutkimuksesta, joka koskee mainepohjaisia suojattuja reititystekniikoita ad hoc -verkoissa. Esimerkiksi Marti et. al [40] ehdottavat turvalliseksi reititystekniikaksi kaksitasoista moduulikehystä. Tämä kehys hyödyntää "vahtikoira"-moduulia (engl. *watch dog*) maineen ylläpitoon ja "polunarvioija"-moduulia (*pathrater*) maineinformaation soveltamiseksi reititykseen. Samanlaista kaksimoduulista kehystä voidaan käyttää DSS:ssä: yksi maineen ylläpitämiseen ja toinen maineinformaation soveltamiseen datafuusiossa fuusiokeskuksessa. [10]

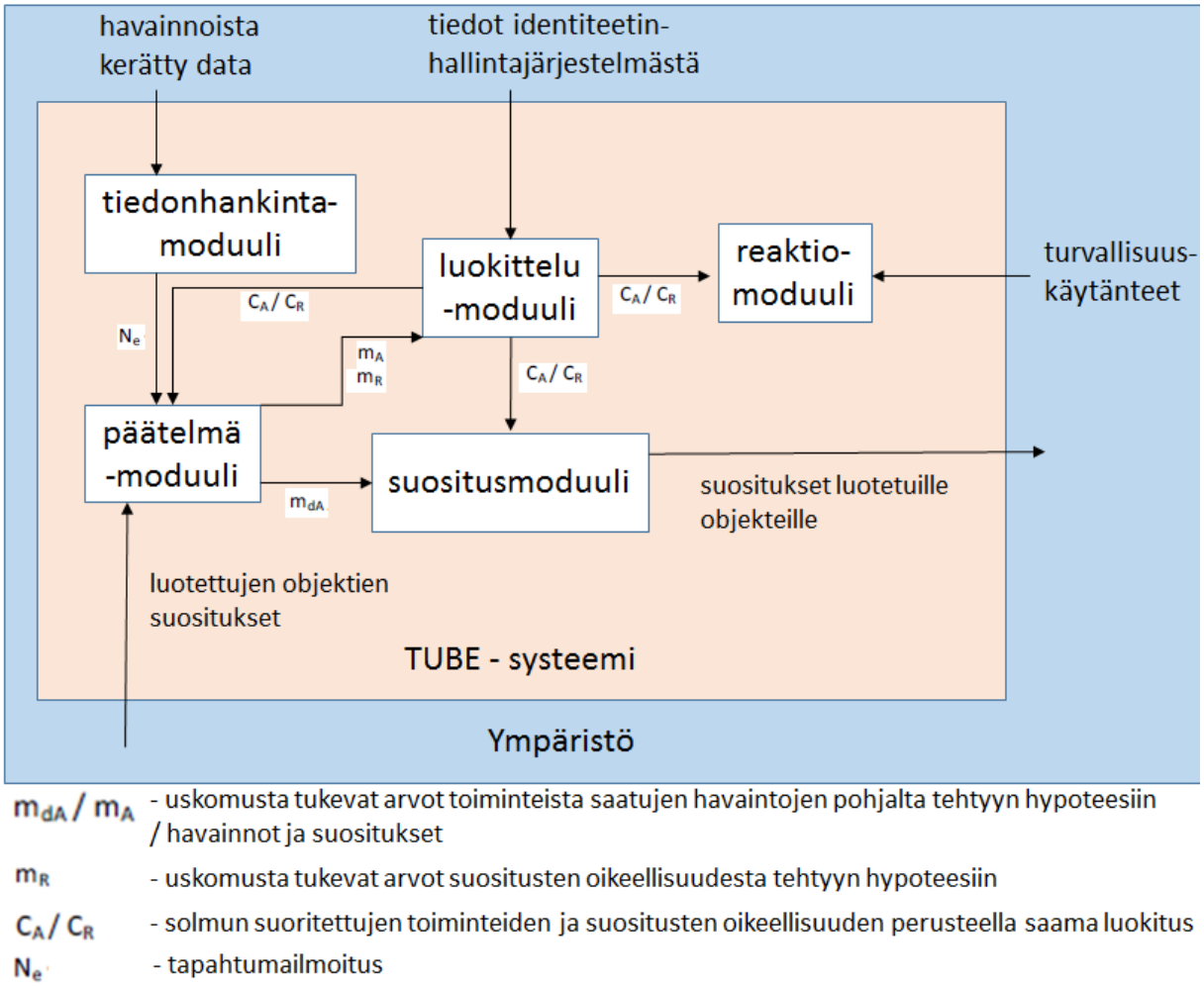
Edellä mainitussa kaksitasoisessa moduulikehyksessä ensimmäisessä moduulissa mainearvio annetaan jokaiselle anturipäätteelle paikallisen havaintoraportin tarkkuuden perusteella, mikä arvioidaan suhteessa fuusiokeskuksen lopulliseen mittauspäätökseen. Toisessa moduulissa tiedonkerääjä hyödyntää mainearviointia arvioidessaan jokaiselta anturipäätelaitteelta vastaanotetun paikallisen taajuuksien havaintoraportin luotettavuuden. [10]

Yhteenvetona voidaan tulkita, että solmujen luotettavuuden arviointitekniikat tulee olla kiinteä osa kognitiivista tietoliikenneverkkoa. Solmut vaihtavat keskenään kriittisiä signalointiviestejä, joita tarvitaan tietämyksen lisäämiseksi spektriympäristöstä tai tukemaan dynaamista taajuuksien käyttöoikeutta ja hallintaa (esimerkiksi kognitiivinen reititys, topologian hallinta). Jos todennetun solmun kognitiivinen moottori yrittää lähettää vääriä tietoja (esimerkiksi havaintojen tuloksista), muu verkko voi romahtaa kokonaan. [1, kpl 4 s. 35] Luotetut ja epäluotetut solmut tulee ottaa huomioon reititysvalinnassa, ja epäluotetut solmut tulee kyetä poissulkemaan järjestelmästä. Tästä syystä sotilaallisissa kognitiivisissa Ad hoc -verkoissa NATO:n tutkimusraportissa [1] ehdotetaan käyttöön otettavaksi tekniikan, joka on nimetty luottamuspohjaiseksi tilannevaroitusjärjestelmäksi (*TUBE, TrUst-Based situation awarEness system).*

3.6.2 TUBE - luottamuspohjainen tilannevaroitusjärjestelmä

TUBE-järjestelmä suorittaa kolmea päätoimintoa: kerää ympäristötietoa, arvioi solmujen luotettavuutta ja ehdottaa reaktioita tunnistettuihin uhkiin. Se koostuu seuraavista moduuleista (kuva 12): [1, kpl 4, s. 35-37]

- tiedonhankintamoduuli
- päätelmämoduuli
- suositusmoduuli
- luokittelumoduuli
- reaktiomoduuli



m_{dA} / m_A - uskomusta tukevat arvot toiminteista saatujen havaintojen pohjalta tehtyyn hypoteesiin / havainnot ja suositukset

m_R - uskomusta tukevat arvot suositusten oikeellisuudesta tehtyyn hypoteesiin

C_A / C_R - solmun suoritettujen toiminteiden ja suositusten oikeellisuuden perusteella saama luokitus

N_e - tapahtumailmoitus

Kuva 12. TUBE-järjestelmän arkkitehtuuri sotilaallisia kognitiivisia Ad Hoc -verkkoja varten [1, kpl 4 s. 36]

Ympäristön arviointi suoritetaan seuraamalla jatkuvasti naapurikohteiden käyttäytymistä. Kuitenkin useassa tapauksessa yhden elementin hankkima tieto on riittämätöntä oikean tilanneymmärryksen syntymiseksi. Siksi tarvitaan tiedonvaihtoa muiden luotettavien kohteiden välillä. Lisätietoja kohteen suojausominaisuuksista saadaan identiteettihallintajärjestelmästä. Kohteen luokittelussa käytetään edistynyttä päätelmätekniikkaa, joka perustuu turvallisuuskäytänteisiin. Tätä luokittelua tarvitaan reititysohjausmekanismien mukauttamiseksi ja havaittujen uhkien vaikutusten vähentämiseksi. [1, kpl 4, s. 35-37]

TUBE-järjestelmän arkkitehtuurissa tiedonhankintamoduulin vastuulla on siepata ja analysoida kognitiivisia signalointiviestejä sekä tehdä alustava arvio tapahtumista. Kohteen käyttäytymisen arviointi perustuu solmujen vaihtamien signalointiviestien paikkansapitävyyteen ja kohteen yhteistyöhön signalointiviestien välittämisessä. [1, kpl 4, s. 35-37]

Päätelmämoduulin vastuulla on kohteiden arviointi suorien havaintojen ja suositusten perusteella. Suositukset voivat olla kuitenkin puolueellisia tai vanhentuneita, joten ne pitää varmentaa ennen niiden käyttöä luokittelutarkoitukseen. Moduuli suorittaa seuraavia funktioita: [1, kpl 4, s. 35-37]

- suora arviointi perustuen suoritettuihin toimintoihin
- suositusten varmentaminen
- suora arviointi liittyen suositusten paikkansapitävyyteen
- suoritettujen toimintojen arviointi perustuen sekä havaittuihin toimintoihin että varmennettuihin suosituksiin

Hälytyksen toiminnasta, jossa on havaittu epänormaalia käyttäytymistä, voi laukaista erilaiset tapahtumat. Lisäksi syötteenä tuleva data voi olla epäluotettavaa, epätäydellistä ja ristiriitaista, mistä syystä on päätetty käyttää Dezertin ja Smarandachen päätelmä- ja luokitteluprosesseja [41]. Tämä sallii joukon primaarisia ja toissijaisia hypoteeseja, joilla määritetään solmun käyttäytymistä, mikä parantaa mahdollisten uhkien havaitsemisen laatua. Jos kyseessä on suora suoritettuihin toimintoihin perustuva arviointi, sen yhteydessä tarkastellaan seuraavia hypoteesiryhmiä: yhteistyöhaluinen, epävarmasti yhteistyöhaluinen, itsekäs, epäillysti itsekäs, rehellinen, epävarmasti rehellinen, valehtelija ja epäillysti valehtelija. [1, kpl 4, s. 35-37]

Päätelmämoduuli suorittaa seuraavan funktion mukaisen laskutoimituksen jokaista hypoteesia varten: [1, kpl 4, s. 35-37]

$$m_b(x_1) = \frac{\sum_k w_k \cdot n_{1k}}{\sum_k w_k \cdot \sum_i^{|D^\Theta|} n_{ik}},$$

missä:

- m_{dA} (x_1) - hypoteesin x_1 uskomusta tukevat arvot

- $D^\Theta = \{x_1, x_2, \ldots, x_N\}$ - kaikkien hypoteesien joukko, missä $| D^\Theta | = N$;

- n_{ik} = tapahtumien lukumäärä, joka arvioidaan x_i:na k:ssa aikavälissä; ja

- w_k - tapahtuman painokerroin k:lla aikavälillä.

Monissa tapauksissa yhden kohteen hankkima tieto on riittämätöntä nykyisen tilanteen kokonaisvaltaiseksi arvioimiseksi. Siksi on tarpeen vaihtaa tietoja muiden verkon luotettavien komponenttien kanssa. Tämän toiminnon suorittaa suositusmoduuli. Suositukset lähetetään määräajoin käyttämällä erillistä protokollaa. Ne sisältävät m_{dA} () -arvot jokaiselle hypoteesille ja aikaleiman. [1, kpl 4, s. 35-37]

Sotilaallisessa kontekstissa luotetut kohteet voivat muuttaa käyttäytymistä tiettyjen tavoitteidensa saavuttamiseksi tai koska ne ovat joutuneet vastustajan haltuun, minkä seurauksena ne voivat lähettää vääriä suosituksia. Suositusten paikkansapitävyyden tarkastaminen ja valheellista tietoa tuottavien solmujen havaitseminen on monivaiheinen prosessi, joka suoritetaan suorista havainnoista, suosituksista, historiatiedoista, todennusmekanismista ja solmun sijaintia koskevista tiedoista johdetun tiedon perusteella. [1, kpl 4, s. 35-37]

Päätelmämoduuli hylkää itseään mainostavat suositukset ja epäluotettavien kohteiden lähettämät suositukset. Moduuli vahvistaa vastaanotetut suositukset kertyneen tiedon perusteella. Jos tällaisia tietoja ei ole saatavilla, päätös vastaanotetun suosituksen vahvistamisesta tehdään lähettämällä kohteen luokitus suositusten paikkansapitävyyden suhteen. Jokainen vahvistettu suositus myötävaikuttaa siihen liittyvän kohteen arviointiin. Suosituksen paikkansapitävyyttä koskevan suoran arvioinnin aikana otetaan huomioon seuraavat kohteeseen liittyvät hypoteesit: rehellinen, epävarma rehellinen, epäilty valehtelija tai valehtelija. Kunkin hypoteesin m()-arvo suositusten paikkansapitävyydestä riippuu hypoteesia vastaavien tapahtumien lukumäärästä, tapahtumien aikaleimasta ja tapahtumien suhteellisesta painotuksesta (esimerkiksi epätavanomaisilla tapahtumilla on suurempi painoarvo, kuin tavanomaisilla). Kohteen arviointiin sisällytetään suositukset, jotka ovat kertyneen tiedon mukaisia tai johdettu luotettavista solmuista. Klassista DSm-yhdistelmäsääntöä käytetään suorien toimien ja suositusten suoran arvioinnin sulauttamiseen. [1, kpl 4, s. 35-37]

Luokittelumoduuli on vastuussa kohteiden lopullisesta arvioinnista identiteetinhallintajärjestelmästä saatujen tietojen ja suoran arvioinnin tulosten perusteella. Kohteet luokitellaan suositusten paikkansapitävyyden suhteen rehellisiksi tai valehtelijoiksi ja suoritettujen toimien perusteella liittolaisiksi, kumppaneiksi, itsekkäiksi tai haitallisiksi. Luokittelun tulokset edistävät merkittävästi kognitiivisen verkon tilannearviointia, ja niitä voidaan hyödyntää reaktiomoduulissa tarkoituksenmukaisen toiminnan aikaansaamiseksi, mikä voi vähentää havaittujen uhkien vaikutusta. [1, kpl 4, s. 35-37]

NATO:n tutkimustyhmä on testannut TUBE-järjestelmän tehokkuutta ja toimintavarmuutta monimutkaisten hyökkäyksien suhteen Riverbed Modeler -simulaatiotyökalulla. Testissä tavallinen WLAN-solmu laajennettiin sisältämään TUBE-moduulit, ja monihyppylähetykseen käytettiin vakiokonfiguraatiollaan olevaa OLSRv1-reititysprotokollaa. Tiedonhankintamoduuli pystyi keräämään tietoja signalointiviestien välittämisen oikeellisuudesta. Suositusten levittämiseen käytettiin omaa UDP-pohjaista maineenlevitysprotokollaa. Kokeessa solmut arvioivat ympäristönsä 30 sekunnin välein, kun taas suositukset levitettiin 60 sekunnin välein. Kokeessa keskityttiin väärin käyttäytyvien solmujen havaitsemiseen, TUBE-järjestelmän robustisuuteen valittujen hyökkäysten suhteen sekä järjestelmän tehokkuuden arviointiin. Testi osoitti, että TUBE:n reaktiomoduuli ottaa huomioon molempien luokittelujen tulokset ja mukauttaa tiedonsiirron ohjausmekanismeja verkon turvallisuuden parantamiseksi ja viestinnän tehostamiseksi. Tulokset vahvistavat, että TUBE-järjestelmän toteuttaminen kognitiivisissa radioverkoissa voi vähentää merkittävästi haitallisten kognitiivisten kohteiden myötävaikutusta sotilaallisissa kognitiivisissa Ad Hoc -verkoissa. [1, kpl 4, s. 35-40]

4. ASIANTUNTIJAKYSELY KOGNITIIVISISTA TIETOLIIKENNE-JÄRJESTELMISTÄ JA NIIHIN KOHDISTUVISTA KYBERUH-KISTA

4.1. Kyselyn toteutus

Kysely toteutettiin delfoi-menetelmää hyödyntäen. Kosolan ja Pasivirran mukaan delfoita käytetään usein näkemysten ja ideoiden esille tuomiseksi suunnittelun ja päätöksenteon pohjalle. Menetelmä on osoittautunut käyttökelpoiseksi, mikäli tarkasteltavan ongelma-alueen asiantuntijoita on vähän, tai heitä ei esimerkiksi ajanpuutteen takia saada saman suunnittelupöydän ääreen. Lisäksi menetelmässä ei vastaajien asema tai muu vastaava tekijä saa liiallista dominanssia vastaajien suhteen. [42, s. 114–115]

Menetelmän keskeisiä onnistumisen edellytyksiä ovat anonymiteetti ja argumenttien iteraatio. Delfoissa on kaksi tai useampia iteraatiokierroksia, joista ensimmäisellä on tarkoituksena kerätä mahdollisimman laaja erilaisten näkemysten massa. Toisella kierroksella karsitaan ensimmäisellä kierroksella esiin tulleista tutkimusongelmaan liittyvistä argumenteista oleellisimmat, jotka valitaan jatkotarkasteluun. Menetelmän onnistumisen edellytyksenä on myös se, että valittu asiantuntijaryhmä tuntee asetetut kysymykset ja kykenee muodostamaan niistä oikeansuuntaisen mielipiteen. Mielipiteen tulee vastata heidän näkemystään tutkittavaan ongelmaan. [42, s. 114–115]

Kyseessä on empiirisen tutkimuksen perusmuotoinen kuvaileva eli deskriptiivinen tutkimusmuoto. [3, s. 14] Kyselylomakkeita ja Delfoin iteraatiokierroksien luonnetta voidaan kuvailla kvantitatiiviseksi, sillä niiden vastauksia analysoimalla kyetään vastaamaan tietotarpeeseen siitä, mitä yksittäisiä asioita vastaajat pitävät tilastollisesti tärkeimpinä kognitiivisessa tietoliikennejärjestelmässä. Aineistonkeruumenetelmänä on käytetty sekä avointa että strukturoitua mallia, ja siten vastauksien analysointiakin toteutettu sekä kvalitatiivisen, että kvantitatiivisen sisällönanalyysin avulla. Kvalitatiiviset ja kvantitatiiviset tutkimusmenetelmät voivatkin täydentää toisiaan. Laadullinen tutkimus laajentaa ja syventää kvantitatiivisen analyysin numeerisia tuloksia esimerkiksi haastatteluaineistojen avulla. [43]

Delfoi-kysely toteutettiin kahdessa kierroksessa. Ensimmäisellä kierroksella vastaajat saivat vapaamuotoisesti ilmaista omat näkemyksensä kognitiivisen tietoliikennejärjestelmän ominaisuuksista, haavoittuvuuksista sekä turvallisuutta parantavista seikoista. Ensimmäisen kierroksen avoimiin kysymyksiin saatuja vastauksia analysoitiin vertaamalla niitä kvalitatiivisessa kirjallisuusselvityksessä esiin nousseisiin keskeisiin teoreettisiin näkökohtiin. Aineiston luokittelurunko sai siis selkeitä virikkeitä kirjallisuudesta, mikä tuo analyysiin vahvan teoriaohjaavan sävyn. Tuomen ja Sarajärven [6] mukaan teoriaohjaavassa analyysissä analyysi ei pohjaudu suoraan teoriaan, mutta teoria voi toimia apuna analyysin toteuttamisessa. Aikaisempi tieto on havaittavissa, mutta sen rooli on enemmänkin uusia ajatusuomia herättävä kuin aiempaa tietoa testaava. Päättelyn logiikka on teoriaohjaavassa analyysissä määriteltävissä abduktiiviseksi; tutkijan ajattelussa vaihtelevat valmiit mallit sekä aineisto. [6, s. 109-111] Aineistoa luokiteltiin vastausten esiintyvyyden perusteella ja tehtiin havaintoja siitä, mitä kokonaisuuksia ei ollut kirjallisuusselvityksen perusteella tullut ilmi. Analyysin etenemistä kuvataan kyselykohtaisesti tarkemmin luvuissa 4.2 ja 4.3.

Toista kierrosta varten ensimmäisen kierroksen analysoitujen vastausten sekä kirjallisuusselvityksessä esiin nousseiden teoreettisten ajatusten pohjalta laadittiin strukturoituja väittämiä. Väittämien vastausvaihtoehdot noudattelivat muutamaa poikkeusta lukuun ottamatta Likertin 5-portaista asteikkoa. Kognitiivista radiota ja tietoliikennejärjestelmää kuvaavissa väitteissä Likertin asteikon ääripäät (1 ja 5) olivat kuvattu vaihtoehdoilla ”täysin samaa mieltä” sekä ”täysin eri mieltä”. Vastaavasti kognitiiviseen tietoliikennejärjestelmää vastaan kohdistuvia uhkia kuvaavissa väitteissä vastausvaihtoehdot olivat ”erittäin merkittävä uhka” sekä ”ei merkittävää uhkaa”. Kolmannessa osiossa kognitiivisen tietoliikennejärjestelmän kyberturvallisuutta parantavissa toteutusvaihtoehtoväittämissä vastausvaihtoehdot olivat ”erittäin suuri merkitys” sekä ”ei merkitystä”. Viimeinen osio käsitteli muita esiin nousseita, erityisesti taktiseen kognitiiviseen tietoliikennejärjestelmään kohdistuvia vaatimusväittämiä, joissa vastausvaihtoehdot olivat ”erittäin tärkeä vaatimus” ”ei tärkeä vaatimus”. Muiden vastausvaihtoehtojen (2, 3 ja 4) sanalliset kuvaukset olivat jätetty kokonaan pois. Näin ollen vastaajilta pyrittiin estämään mahdollisuus harkitsemattomaan vastaukseen. [44, s. 53] Muutamassa kysymyksessä, jossa haluttiin verrata vaihtoehtojen painotuksia keskenään, oli valintavaihtoehdot monivalintakysymyksiä tai vaihtoehdoilla ”kyllä” ja ”ei”.

Toisen kierroksen vastaukset analysoitiin kvantitatiivisesti. Vastaukset luokiteltiin vastausvaihtoehtojen suhteellisten prosentuaalisten jakaumien perusteella kolmeen eri kategoriaan: merkittävän konsensuksen saaneisiin väittämiin, osittaisen konsensuksen saamiin väittämiin sekä ei konsensusta saaneisiin väittämiin. Asiantuntijoiden vastausten kvantitatiivisen analyysin perusteella väittämien tuloksista pystyttiin tekemään johtopäätöksiä eri kokonaisuuksien paikkansa pitävyydestä sekä tärkeydestä.

Kysely lähetettiin kahdelletoista Puolustusvoimien, tiedeyhteisön sekä teknologiateollisuuden aihealueen asiantuntijalle. Heistä tutkimukseen osallistui seitsemän asiantuntijaa, jotka on esitelty liitteessä 2. Tässä tutkimuksessa ei otettu kantaa vastaajien taustamuuttujiin (kuten organisaatio), koska pienestä perusjoukosta johtuen haluttiin säilyttää vastausten anonymiteetti.

4.2. Kyselyn ensimmäinen kierros

Kyselyn ensimmäinen kierros sisälsi avoimia kysymyksiä tutkimuksen pääkysymykseen ja alakysymyksiin liittyen. Lisäksi kyselyn lopussa oli annettu mahdollisuus avoimiin kommentteihin. Kysymyksiä laadittiin kahdeksan kappaletta:

- 1. Millaiset ominaisuudet mielestäsi tekevät tietoliikenneverkosta kognitiivisen?
- 2. Kognitiivinen radioverkko koostuu solmuista, joista löytyy kognitiivinen radio. Mitä ominaisuuksia/toiminnallisuuksia tämä radio voisi sisältää?
- 3. Mitä kognitiivisia ominaisuuksia taktiseen radioverkkoon voisi kuulua?
- 4. Mitä hyötyjä tai uhkia kognitiivisuus tietoliikennejärjestelmissä voisi muodostaa sotilaallisessa kontekstissa?
- 5. Millaisia kyberuhkia voisi kohdistua kognitiiviseen tietoliikenneverkkoon?
- 6. Suurvallat käyttävät termiä Cyber-EW, jolla tarkoitetaan elektronisen sodankäynnin integroitumista kyberulottuvuuden kanssa. Millaisia uhkia tämänkaltaiset hyökkäysvektorit voisivat aiheuttaa kognitiiviselle radioverkolle?
- 7. Mitä vaatimuksia kyberturvallisuuden suhteen tulisi asettaa nimenomaan kognitiiviselle tietoliikenneverkolle?
- 8. Millaisia toteutusvaihtoehtoja kognitiivisen tietoliikenneverkon kyberturvallisuuden parantamiselle voisi löytää?

Kyselyn ensimmäiseen kierrokseen vastasi kuusi henkilöä, vastausprosentin ollessa 50%. Tästä eteenpäin vastaajien anonymiteetin säilyttämiseksi referoin vastaajia kirjaimilla A, B, C, D, E ja F.

4.3. 1. kierroksen tulosten analysointi

Kysymykseen ”1. Millaiset ominaisuudet mielestäsi tekevät tietoliikenneverkosta kognitiivisen?” liittyen kaikki vastaajat mainitsivat automaattiset toiminnot, jotka ohjaavat verkon toimintaa. Automaattisuuteen liittyviin toimintoihin vastaajat listasivat seuraavia ominaisuuksia:

- Verkon suunnittelu (n = 1)
- Verkon havainnointi (n = 3)
- Verkon adaptiivisuus toimintaympäristön tai vaatimusten mukaan (n = 4)
- Verkon optimointi (n = 3)
- Kognitiivista verkkoa ja sen toimintaa / toiminnallisuuksia tulisi kyetä kuitenkin valvoa ja hallita ihmisen toimesta (n = 1)

Verkon suunnitteluun liittyen vastaajan A havainto siitä, että kognitiivisuus automatisoi verkon suunnittelua ja hallintaa, tukee kappaleessa 2 tehtyjä havaintoja kognitiivisuuden mahdollisuuksista johtamisjärjestelmien suunnittelun ja hallinnan helpottamiseksi operaatioiden toimeenpanemisessa. Vastauksessa tulee kuitenkin ilmi, että suunnitteluperusteet tulee edelleen luoda manuaalisesti.

Verkon havainnointiin liittyen vastauksista ilmenee liikenteen määrän havainnointi, jonka perusteella voidaan optimoida verkon toimintaa seuraavin keinoin: uudelleenohjaus, liikenteen katkaisu tai liikenteen priorisointi (B). Havainnointiin liittyen tulisi tekoälyavusteisesti löytää liikenteen säännönmukaisuuksia, joiden avulla verkko voi oppia syy-seuraussuhteita liikenteen suhteen (D). Havainnoinnin perusteella toteutettavat toiminnot perustuvat ennalta määriteltyihin sääntöihin (B).

Vastauksien perusteella verkon adaptiivisuus ja optimointi voi tapahtua yksittäisten solmujen välillä (A), mutta koko verkon ollakseen kognitiivinen tulee adaptiivisuudella ja optimoinnilla käsittää koko verkon laajuista toimintaa (C). Tämä optimointi voi perustua älykkääseen parametrien hakuun (A). Vastaajat A ja D ottivat kantaa myös siihen, että adaptiivisuuden ja optimoinnin suhteen tehtävän ja operaation suoritusvaiheen tulisi vaikuttaa haluttuun lopputulokseen (tilannekuva, salaaminen, harhauttaminen, tiedustelu, tulenjohto, häirinnän väistö, kokonaissuorituskyky).

Kysymyksen ”2. Kognitiivinen radioverkko koostuu solmuista, joista löytyy kognitiivinen radio. Mitä ominaisuuksia/toiminnallisuuksia tämä radio voisi sisältää?” vastauksista löytyy seuraavia ominaisuuksia:

- Radion kyky havainnoida taajuusspektriä sekä liikennettä (n = 4)
- Kyky lähettää ja vastaanottaa laajalla taajuusspektrillä (n = 3)
- Kyky toimia myös elektronisen tiedustelun ja vaikuttamisen (häirintä) suhteen (n = 2)
- Taajuushypytys (n = 2)
- Antennien ohjaaminen (n =1)
- Hyötylähetteiden releointi (n = 2)

Radion kyvykkyysvaatimukset taajuusspektrin sekä tietoliikenteen havainnoinnin suhteen tukevat kappaleessa 2.1 tehtyjä havaintoja. Tutkimuksessa uusina havaintoina kantaa otettiin erityisesti radioiden kykyyn toimia sensoreina ja häirintälähettiminä tarvittaessa. Vastaaja D esitti, että radion olisi kyettävä häirintälähettimenä toimiessaan lähettämään viholliselle autenttisen oloista liikennettä. Kun radiolla ei lähetetä, tulisi sen kyetä toimimaan sensorina niin omille lähetteille (esim. radiohiljaisuus) kuin vihollisen lähetteille (ELTI) (B). Elektronisen suojautumisen näkökulmasta radion tulisi kyetä havaitsemaan häirintä, ja väistämään sitä tehosäätelyllä tai muiden keinojen avulla (taajuushyppely / kaistanvaihto / varakanavat) (B)

Taajuus-spektrin suhteen antennien sekä radion olisi kyettävä hyödyntämään mahdollisimman laajaa taajuuskaistaa (UHF, VHF, HF) (B). Radion tulisi kyetä myös lähettämään niin salattua kuin salaamatonta liikennettä, sekä useita erilaisia lähetteitä (esim. ääni, IP, salattu IP) (B). Kontrolliliikenteen tarve ilmenee havainnossa, jossa radioiden on kyettävä neuvottelemaan käytetty taajuusalue (B). Kognitiiviseen radioverkkoon tulisi pystyä lisäämään myös vanhemman sukupolven ei-kognitiivisia ohjelmistoradioita, joille kognitio voi antaa rajattuja ohjauskomentoja ja asettaa rajoitetusti tiedonsiirtoparametreja (E) [45].

Kirjallisuusselvityksessä järjestelmän antenniratkaisuihin ei oltu otettu kantaa. Sen suhteen vastauksissa ilmeni tärkeä havainto siitä, että radiolla tulisi olla kyky ohjata radion antenneja (A). Kuten edellä kävi ilmi, tulisi laajasta taajuusspektristä johtuen antenneja olla useanlaisia, ja osa niistä olisi suunta-antenneja. Mikäli radio ei automaattisesti ohjaa näitä antenneja, menetetään automatiikan hyödyt. Antennien ohjaustieto voi yksinkertaisimmillaan olla esimerkiksi MATI:sta saadun paikkatiedon hyödyntämistä, minkä perusteella radio pyörittää antennia (A).

Vastaaja A oli sitä mieltä, että paras suorituskyky saataisiin silloin, kun esimerkiksi M18-järjestelmässä ohjaus tehdään verkon hallintatyökalulla Node Managerista tai radiosta suoraan. Ohjaus perustuisi radioparametrien hyödyntämiseen verkon muodostamisvaiheessa ja myöhemmin koko verkon suorituskyvyn optimoimiseen (A). Tekoälyavusteinen verkon hallintasovellus (esimerkiksi tekoälyavusteinen Network Manager) voi suunnitella verkon rakenteen vastaamaan haluttua verkon suorituskykyä, kieltää huonot naapuruudet ja poistaa tarpeettomat yhteydet, minkä avulla verkko voidaan rakentaa minimipalveluista täyteen suorituskykyyn (A). Tekoäly voi huomioida myös vihollisen hallussa olevan ryhmityksen ja kieltää lähetyksen ja vastaanottamisen sieltä suunnasta (A). Järjestelmään liitetyssä kenttäradioissa lähetystehoa ja antennin sähköistä pituutta muuttamalla solukoko voidaan optimoida suojautumisen tai suorituskyvyn perusteella (A).

Kysymyksen ”3. Mitä kognitiivisia ominaisuuksia taktiseen radioverkkoon voisi kuulua?” vastauksista löytyi seuraavia ominaisuuksia:

- Verkon kyky havainnoida taajuusspektriä sekä liikennettä (n = 3)
- Kyky jakaa näitä havaintoja muiden solmujen kanssa ja muodostaa sitä kautta kattavampi kuva toimintaympäristöstä ja päätöksentekoa varten (n = 2)
- Kyky tunnistaa lähetekuvioita ja toimijoita verkossa sekä visualisoida havainnot ihmisen tulkinnan helpottamiseksi (n = 1)
- Kyky taltioida havainnot kirjastoon ja oppia havaintojen pohjalta (työmuisti ja herätekirjasto) (n = 1)
- Solmut vastaanottavat komentoja muilta verkon solmuilta tai verkon hierarkiassa korkeammalla olevilta solmuilta (n = 1)
- Kyky verkon laajuiseen häirinnän väistämiseen sekä vihollisen asemien paikallistamiseen (n = 2)
- Kyky valita paras siirtotie ilman käyttäjän valintaa (n = 1)
- Kyky generoida asemakäskyt automaattisesti (n = 1)
- Kyky laitetason ongelmanratkaisuun ja päätöksentekoon autonomisesti (n = 1)
- Mahdollisuus käyttäjän hyväksyntään verkon rakenteen muutoksissa (n = 1)
- Kyky toimia yllättävästi, esim. vastustajan taajuuksia käyttäen (n = 1)

Edellä mainitut asiat noudattelevat pitkälti kappaleessa 2 tehtyjä havaintoja siitä, että verkolla tulee olla verkon kattava kyky havainnoida taajuusspektriä ja tietoliikennettä, sekä kyky jakaa näitä havaintoja muiden solmujen kanssa (jaettu taajuushavainnointi DSS). Myös havainto komentojen välittämisestä verkossa liittyy kappaleissa 2 ja 3 esitettyyn kontrollikanavan (tai -kanavien) tarpeellisuuteen. Sotilaallista kontekstia vastauksissa edustaa edelleen vahva elektronisen sodankäynnin suorituskyvyn parantaminen niin elektronisen suojautumisen (häirinnän väistö) kuin elektronisen tiedustelun (vihollisen suuntiminen ja paikantaminen) suhteen kognitiivisten ominaisuuksien avulla. Myös vastaajan F lisäys siitä, että radioverkon tulisi kyetä toimimaan yllättävästi, esimerkiksi vihollisen käyttämän taajuusalueen hyödyntämisellä, tukee laajentuneita taktisia käyttöperiaatteita.

Kirjallisuusselvityksessä ilmentymättömiä aihekokonaisuuksia edusti ehdotus tekoälyn kyvystä muodostaa havainnoista käyttäjä helpommin tulkittavissa olevaa dataa visuaalisen käyttöliittymän avulla, jolloin myös käyttäjä pysyy helpommin tilannekuvan tasalla. Tämä liittyy osittain myös vastaajien A ja B ensimmäisen ja kolmannen kysymyksien vastausten vaatimuksiin integroida järjestelmään ominaisuus, joka mahdollistaa ihmisen päätöksenteon viimeisenä hyväksyjänä kognitiivisten päätösten toimeenpanossa.

Myös yksi käytännön ehdotus operaation toimeenpanoa helpottamaan oli vastaajan A vaatimus siitä, että tekoäly kykenisi generoimaan suunnitellun toiminnan vaiheisiin sidotut asemakäskyt, jotka käsketään järjestelmälle suunnitteluvaiheessa offline-tilassa tai toiminnan aikana verkon yli. Vastaaja A korosti, että tämä prosessi tulee olla huolellinen, jotta asemamiehistön ja tekoälyn välille ei tule toteutusristiriitaa automatiikan, aseman tehtävän ja asemakäskyn ihmisen luettavan osuuden välille.

Kysymyksen ”4. Mitä hyötyjä tai uhkia kognitiivisuus tietoliikennejärjestelmissä voisi muodostaa sotilaallisessa kontekstissa?” vastauksissa esiintyi seuraavia hyötyjä:

- Taistelukentän olosuhteisiin autonomisesti adaptoituva ja toiminnan optimointiin soveltuva tietoliikenneverkko (n = 2)
- Suorituskyvyn paraneminen siviilitoimintaympäristöä haastavammissa olosuhteissa (n = 3)
- Verkon toiminnan mukautuminen autonomisesti erilaisiin toimintamoodeihin taktisen tilanteen mukaan (n = 1)
- Verkon suunnittelun ja operaation aikaisen toimeenpanon automatisointi (n = 1)
- Kognitiivisuuden myötä myös tieto saavutettavuudesta paranee, sillä voidaan olettaa, että saatu viesti kuitataan ns. laitetasolla, jolloin verkolla on myös tieto siinä toimivista laitteista ja niiden käyttäjistä (n = 1)

Kuten kappaleessa 2.4 on esitetty, suurimmat haasteet sotilaallisissa tietoliikenneverkoissa aiheutuvat siviiliympäristöä haastavammasta toimintaympäristöstä, verkon jatkuvista muutoksista ja vihollisen tahallisesta häirinnästä. Vastaukset noudattelivat näiltä osin saavutettuja hyötyjä erityisesti spektrin paremman hyötykäytön (laajempi kaistanleveys), muuttuvissa tilanteissa verkon optimoinnin sekä vihollisen häirinnän sietokyvyn kasvamisen osalta.

Taktista näkökulmaa edusti erityisesti vastaukset verkon suunnittelun ja toimeenpanon automatisointiin liittyen. Sotilaallisten tietoliikenneverkkojen monimutkaistuessa johtamisjärjestelmästä vastaavan johtamisjärjestelmäpäällikön tehtäväkenttä on muuttunut erittäin haastavaksi. Vastaaja A on maininnut mahdollisia hyötyjä niin operaation suunnitteluvaiheessa kuin sen aikana: ”Tekoälypohjainen suunnitteluohjelma kykenisi laskemaan tausta-ajona neuroverkkolaskennalla ensin pienemmät toiminta-alueet ja sitten operaatioalueet, jolloin vastaus verkkosuunnitteluun tulee välittömästi. Tekoäly kykenee rakentamaan tausta-aineiston perusteella optimaalisen verkon. Tässä pohja-aineistona tulee olla operaation aikatekijät, jotta solmut siirtyvät niihin paikkoihin, jotka operaatiossa on toteutettu tai suunniteltu. Suunnitelmia lasketaan ja optimoidaan jatkuvasti operaatiovaiheiden edetessä. Näiden perusteella rakennetaan automaattiset asemakäskyt laitteille ja paperiset ja sähköiset asemakäskyt asemille ja asioita toimeenpaneville johtajille.”

Edellä mainittujen ominaisuuksien todellinen hyödyntäminen vaatisi vastaajan A mukaan MATI:n ja verkon tekoälyn välille rakennettua rajapintaa, jonka avulla mahdollistetaan minimi määrä informaation vaihtoa järjestelmien välillä datana, johtamissanomina tai vastaavana, jotta päästään lähes reaaliaikaiseen toteutukseen ja suunnitteluun.

Samoin vastaajan C esille nostamat erilaisten taktisten tilanteiden vaatimat toimintamoodit sekä verkon toiminnan autonominen mukautuminen niihin liittyy kiinteästi taktiikkaan. Tällä hetkellä taktisia toimintatapoja langattomissa sotilasverkoissa edustavat emissiokontrollitasot (EMCON-tasot), joilla ohjataan sähkömagneettista säteilyä lähettävien laitteiden säteilyä, sekä moodiprofiilit, joilla ohjataan eri radioiden lähetteiden parametrejä ja suorituskykyä. EMCON-tasot ja moodiprofiilit eivät ole kytköksissä toisiinsa, ja niiden käytöstä vastaa johtamisjärjestelmäpäällikkö. Näiden toiminnallisuuksien muutokset verkossa vaativat aina suorittavan portaan oikea-aikaisesti tehtyjä oikeita toimenpiteitä, ja inhimillisten virheiden mahdollisuus korostuu. Näiden toiminnallisuuksien integroiminen kognitiiviseen päätöksentekoon ja automatiikkaan tiettyjen ennalta laadittujen sääntöjen pohjalta olisi varmasti hyödyllinen ominaisuus.

Vastaavasti uhkiin liittyen vastaajat listasivat seuraavia asioita:

- Asiantuntijuuden puute järjestelmää suunniteltaessa (n = 2)
- Liiallinen tukeutuminen verkon autonomiseen toimintaan ja sen seurauksena järjestelmän kontrollin menettäminen, tai unohdetaan huolehtia siitä, että verkko todella toimii parhaalla mahdollisella tavalla (n = 1)
- Taajuudenvalinta-algoritmin mahdollisia heikkouksia ja niiden hyödyntämistä vastustajan toimesta. Mikäli algoritminen toteutus on vuotanut viholliselle, niin vihollinen voi käyttää tätä hyväksi häiritessään yhteyksiä (n = 2)

Vastauksessa ilmennyt huoli algoritmien vuotamisesta tai murtamisesta vihollisen tiedustelun toimesta liittyy dynaamiseen spektrinkäyttöön (DSA), jota on käsitelty laajemmin kappaleessa 3.2. Algoritmien tietäminen mahdollistaa älykkään elektronisen häirinnän.

Vastauksissa ilmeni myös huoli erityisesti järjestelmän suunnittelu- ja hankevaiheen tarvittavasta asiantuntijuudesta, jotta järjestelmä onnistuu palvelemaan haluttua käyttötarkoitusta. Vastaaja A esitti haasteeksi suunnitteluvaiheessa tarvittavan älykkyyden määrittelemisen ja suunnittelun. Vastaaja D esitti uhkan liittyen asiantuntijuuden puuttumiseen, joka ilmenisi kyvyttömyytenä mallintaa taistelukentän kokonaisuutta ja integroida tietoliikenneverkko siten osaksi koko taistelukentän toimintaa. Huolena oli, että järjestelmän toteutus ei mahdollisesti tee sitä mitä odotettiin, tai sen käyttöliittymä ja toiminnallisuudet eivät ole riittävän helpoiksi suunniteltuja (A).

Suunnittelussa ja määrittelyssä liika monimutkaisuus ja tarpeettomat vaatimukset voivat johtaa mahdollisen toteutuksen kalleuteen, jolloin tekoälyä ei toteuteta tai se toteutetaan vajaasti (A). Lopputuloksena voi olla myös maailman paras kognitiivinen tietoliikennejärjestelmä, joka ei kuitenkaan pysty tukemaan nykyaikaisen taistelukentän kaaoksenomaista toimintaa (D).

Edellä mainittuihin uhkiin liittyen vastaajan A mukaan tulisi varmistua seuraavista asioista: järjestelmän käyttöliittymä ja automatiikka tulisi suunnitella toimimaan keskenään, jotta asemien henkilöstö tietää, että tekoäly tekee heidän puolestaan verkon optimointia ja esimerkiksi vasta-asemat ja laitteiden tehot ja vastaavat asetukset poikkeavat asemakäskystä. Tämä vaatisi järjestelmän käytön prosessien huolellista suunnittelua, koulutusta ja käytön harjoittelua. Tekoälyn tekemät päätökset tulisi tarkastaa järjestelmän ohjaus- ja suunnitteluhenkilöstön toimenpitein. Tekoälylle tulisi antaa päätöksentekokyky pieniin parametrien vaihtoon, mutta tekoälyn tulisi kyetä myös ennalta esitellä merkittävät optimoinnit ja verkkorakenteen muutokset. Tällä varmistutaan siitä, että niihin liittyy sotilaallisen tarkoituksenmukaisuuden tarkastelu sekä teknisen rakenteen optimoinnin seurausten tarkastelu verkon palvelukyvylle. (A)

Myös vastaaja C näki uhkana liiallisen tukeutumisen verkon autonomiseen toimintaan, minkä johdosta voidaan menettää järjestelmän kontrolli tai unohdetaan huolehtia siitä, että verkko todella toimii parhaalla mahdollisella tavalla.

Viidenteen kysymykseen ”5. Millaisia kyberuhkia voisi kohdistua kognitiiviseen tietoliikenneverkkoon?” vastaajat esittivät seuraavia uhkia:

- Hyökkäykset kognitiivista päätöksentekoa vastaan (n = 4)
- Tarvittavien parametrien tekeminen, käsittely, säilyttäminen ja henkilöriskit (n = 1)
- Hyökkäyspinta-alan kasvaminen: esim. verkon topologian muutosalgoritmin ja taajuusvalinta-algoritmin haavoittuvuudet (uudet vaikutusmekanismit) (n = 2)
- Järjestelmään tunkeutuminen, mikä mahdollistaa parametrien korruptoinnin tai ohjelmankoodin muuttamisen (n = 1)
- Tekoälykilpailu (n = 1)
- Normaalit ip-verkon kyberuhkat (n = 1)

Vastaajien kognitiivista päätöksentekoa vastaan kohdistuvien hyökkäysten suhteen oli yhteisiä piirteitä kappaleessa 3.2 ja 3.7 esitettyihin hyökkäysmalleihin. Vastaaja D esitti, että kehittyneempi tekoäly voi vedättää heikompitasoista tekoälyä ja opettaa sille vääriä asioita. Vastaaja C arvioi, että vastapuoli voi oivaltaa, että autonomista kognitiivista verkkoa voi jollain tavalla hämätä tai harhauttaa niin, että se adaptoituu ”väärin” ja tekee jatkuvasti verkon toiminnan kannalta huonoja päätöksiä. Tämä johtaa siihen, että perinteisen radiohäirinnän muoto voi muuttua verkon älykkääksi kohdennetuksi hämäämiseksi (C). Edellä mainittua vaikutustapaa ja suojautumistekniikoita on käsitelty kappaleessa 3.2 ja 3.7. Mielenkiintoinen havainto vastaajalta D oli mahdollinen tekoälykilpailutilanne, jolloin vihollisen tehokkaampi tekoäly voi vedättää heikompitasoista tekoälyä ja opettaa sille vääriä asioita.

Tarvittavien parametrien ja algoritmien tekemiseen, käsittelyyn, säilyttämiseen ja henkilöriskeihin liittyy samoja tietoturvauhkia kuin mihin tahansa tekniseen hankkeeseen. Tähän liittyen hankeprosessit ja hankkeessa mukana olevien muidenkin organisaatioiden tietoturvakäytänteet tulee olla kunnossa.

Mahdollinen järjestelmään tunkeutuminen muodostaa entistä kriittisemmän uhan, koska tunkeutuminen voi tapahtua huomaamattomasti ja tunkeutuja voi manipuloida ohjelmistopohjaista kognitiota mielensä mukaisesti, mikä voi vaikuttaa järjestelmään lamauttavasti (D). Vastaaja B ottaakin kantaa siihen, että käyttäjillä ei välttämättä ole tarkkaa tietoa siitä, mitä verkon tulisi tehdä, jolloin tarkan analyysin (esim. onko tunkeuduttu vai ei) tekeminen on mahdotonta.

Kysymykseen ”6. Suurvallat käyttävät termiä Cyber-EW, jolla tarkoitetaan elektronisen sodankäynnin integroitumista kyberulottuvuuden kanssa. Millaisia uhkia tämänkaltaiset hyökkäysvektorit voisivat aiheuttaa kognitiiviselle radioverkolle?” vastaajat mainitsivat seuraavan laisia uhkia:

- Kognitiivisen radioverkon luotettavuus romahtaa, eikä lähetteisiin voi enää luottaa (n = 1)
- Voi olla mahdollista ohjata radio epäsuotuisalle signaalikaistalle minimoiden sen kaistanleveys, tai jopa katkaista yhteys laajemmassa verkossa (n = 1)
- Kognitiivisuuden tuomat algoritmit luovat lisää monimutkaisuutta ja uusia hyökkäysmahdollisuuksia (n = 2)
- Kognitiivisen verkon reaktioista on mahdollista päätellä, toimiiko häirintä (n = 1)

Verkkoon tunkeutuminen ilmarajapinnan kautta on todennäköisesti erittäin hankalaa, koska on oletettavissa, että verkko on hyvin salattu, ja siinä on muitakin tietoturvaratkaisuja (A ja B). Vastaaja B mainitsee kuitenkin haavoittuvuuden siinä, että kognitiivinen radio joutuu käsittelemään vastaanotetut signaalit, niin on mahdollista, että protokollasta tai vastaavasta löytynyt haavoittuvuus vuotaa kriittistä tietoa (avain, aika, asetukset) vastustajalle mahdollistaen datan purun. Yksinkertaisin keino älykkäälle elektroniselle vaikuttamiselle on kuitenkin hyödyntää kognitiivisen radioverkon automaattisia spektritoimintoja (dynaaminen spektrinkäyttö DSS). Tästä esimerkin mainitsee vastaaja B, joka antaa käytännön esimerkkinä tilanteen, jossa kognitiivinen radio pakotetaan väistämään spektrissä epäsuotuisalle alueelle, eli se pakotetaan esimerkiksi HF-kaistalle tai korkealle UHF-kaistalle, jolloin HF aalto ei saavuta lähikatveessa olevaa vasta-asemaa ja UHF ei etene metsässä. Vastaaja B lisääkin, että kognitiivisen radion vastauksista on myös mahdollista päätellä, tehoaako häirintä vai ei. Edellä mainittuja vaikutusmekanismeja sekä niiltä suojaavia tekniikoita on käsitelty kappaleissa 3.2 ja 3.7. Verkon parametreja suunnitellessa tulisikin huomioida, miten voitaisiin välttää verkon toiminnan perusteella vihollisen häirinnän tehoamisen paljastuminen (B).

Ilmarajapinnan ja elektronisen vaikuttamisen uhkien minimoimiseksi vastaaja A esittää älykkäitä SBA-tyyppisiä antenneja, joiden avulla voidaan parantaa merkittävästi verkon palvelukykyä. Samoin automaattisesti radiosta ohjatut aktiiviantennit optimoivat verkkoa radioiden hypintä- ja taajuus-suunnitelman mukaiseksi vähentäen havaittavuutta ja parhaimmillaan kaksinkertaistaen linkkipituudet. Myös kognitiivisen radion suhteen vastaaja A näkee cyber/EW-elementin enemmän mahdollisuutena kuin uhkana. Koska kognitiivinen radio on tietoinen ympäristöstään ja se kykenee havainnoimaan spektriä tarkemmin kuin aikaisemmat radiot, tarkoittaa se myös kykyä cyber/EW suojautumiseen. (A)

Tätä kykyä voidaan parantaa käyttämällä verkon vapaata kapasiteettiä oman tilannetietoisuuden luomiseen spektristä. Samoja laitteita voidaan käyttää myös hyökkäykseen. Vastustajan vaikuttaminen EW:llä voidaan helposti havaita hypyttämällä vastaanotinta koko taajuusalueella ja samanaikaisesti pyörittämällä sähköisesti keilattavaa antennia, jolloin aseman ympäriltä havaitaan 360-asteen leveydeltä tapahtuva mahdollinen vaikuttaminen. Tieto käsitellään tekoälyllä ja koko järjestelmä suojaa itseänsä kieltämällä vastaanoton kyseessä olevista suunnista. Ympärisäteileviä antenneja käyttävät radiot eivät voi suojautua elektroniselta tiedustelulta tai häirinnältä, mutta tietoisuus vihollisen hyökkäyksestä mahdollistaa vastatoimenpiteiden suunnittelun ja aloittamisen merkittävästi nopeammin kuin nykyisillä järjestelmillä. (A)

Kysymykseen seitsemän: ”7. Mitä vaatimuksia kyberturvallisuuden suhteen tulisi asettaa nimenomaan kognitiiviselle tietoliikenneverkolle?” vastaajat esittivät seuraavia vaatimuksia:

- Varmentavat menetelmät, kuten verkon toimintaa ohjaavien komentojen hallinta ja oikeellisuuden varmistaminen (n = 2)
- Aina salattu yhteys, tarkoin määritetyillä protokollilla ja vaihtoehdoilla mitkä eivät mahdollista salauksen purkamista tai heikentämistä (*degrade*) ilman toimivaa datansiirrollista yhteyttä (n = 1)
- Omien solmujen tunnistaminen (n = 1)
- Tunkeutujien tunnistaminen ja eristäminen (n = 1)
- Mahdollisuus manuaaliohjaukseen protokollien ja yhteydenmuodostuksen saralla sekä käyttäjän mahdollisuus poistaa yhteyksiä ja toiminnallisuuksia (pois lukien salaus) (n = 1)
- Henkilöstön osaamisen kehittäminen (n = 1)
- Tarve päivittää ja evaluoida kognitiivisen verkon suorituskykyä (n = 1)
- NO-toiminnassa vain rajattujen ominaisuuksien käyttömahdollisuus (n = 1)
- Järjestelmän tietoturvaluokkien tarkka määrittely (n = 1)
- Tarkat dokumentoinnit laitevalmistajilta, mikä mahdollistaa kyberturvallisuuden helpomman testaamisen (n = 1)

Verkon toimintaa ohjaavien kontrollikanavien haavoittuvuuksia on käsitelty kappaleessa 3.5 ja 3.6. Niiden yhteenvetona voi todeta, että kontrolliliikenne muodostaa mahdollisen kriittisen haavoittuvuuden yhden pisteen vikaantumiselle ja siksi turvallisuusnäkökulmat on huomioitava. Solmujen välittäminen tietojen oikeellisuuden varmistamiseksi tulee järjestelmään integroida luottamuksenhallintamekanismeja, joilla voidaan rajata ja eristää epäluotettavat solmut.

Sotilastietoliikennejärjestelmät ovat yleensä vahvasti salattuja ja nykyisillä salausprotokollilla voidaan tehdä salauksen purku niin hankalaksi, ettei sillä ole operatiivisen käytön suhteen saavutettavissa hyötyjä. Mikäli verkkoon liittymiseen liittyvät suojaustoiminnot saadaan murrettua tai jokin solmu päätyy toimintakuntoisena vihollisen haltuun, aiheutuu siitä uhkia koko järjestelmälle. Näitä edellä mainittuja uhkia kohtaan tulisi olla mahdollista järjestelmän automaattisesti tunnistaa haitalliset solmut ja saada ne eristettyä muusta verkosta. Esimerkkejä tällaisesta turvallisuutta parantavista vaihtoehdoista on esitelty kappaleessa 3.7 ja 3.8. Vastaajan B ehdotus siitä, että käyttäjälle pitää jättää mahdollisuus manuaaliohjaukseen protokollien ja yhteydenmuodostuksen saralla sekä mahdollisuus poistaa yhteyksiä tai toiminnallisuuksia (pois lukien salaus) tulisi ottaa huomioon turvallisuutta parantavana toimena, mikäli muut mekanismit ovat pettäneet.

Vastaaja F lisäsi, että hankittavien järjestelmien tulee olla testattavissa kyberturvallisuuden suhteen myös antennin kautta. Tämä edellyttää riittävää dokumentaatiota toimittajalta. Pahin tilanne olisi hankittava ”musta laatikko”, jonka toimintaa ei tunneta. Vastaaja A toi esiin haasteet järjestelmän ominaisuuksien tietoturvaluokituksista huolehtimisesta. Kuten tälläkin hetkellä sotilasjärjestelmissä, tulisi järjestelmän normaaliolojen käytön suorituskyky olla rajoittunut järjestelmän todellisista suoritusparametreistä ja suorituskyvyistä (esim. aaltomuodot). Järjestelmän käyttö on tällä hetkellä korkeintaan STIV - vain viranomaiskäyttöön -luokkaa. Useiden järjestelmien ja tekoälyn tuottama data suorituskyvystä voi olla jotain muuta. Tämä tulee etukäteen ymmärtää ja kouluttaa joukko-osastoissa, jotta kaikki ymmärtävät ja käsittelevät tietoa oikein. (A) Myös henkilö D otti kantaa tarpeeseen kehittää henkilöstön koulutusta useilla eri osa-alueilla (erityisesti tekoäly ja mallintaminen).

Kysymykseen kahdeksan: ”8. Millaisia toteutusvaihtoehtoja kognitiivisen tietoliikenneverkon kyberturvallisuuden parantamiselle voisi löytää?” vastaajat esittivät seuraavia toteutusvaihtoehtoja:

- Järjestelmän jatkuva testaaminen, jossa niin sanottu red team yrittää vastustajana heikentää järjestelmän toimivuutta (n = 2)
- Flow ja pakettikaappauksen keskitetty hallinnointi mahdollistaa parhaimman havainnointikyvyn (n = 1)
- Aktiivilaitteiden konfiguraation tiivisteiden jakaminen verkossa mahdollistaa konfiguraatiohallinnan (n = 1)
- Järjestelmän tekoälyn tuottaman datan suojaaminen (n = 1)

Monissa suurissa organisaatioissa on jatkuvaa henkilöstön ja järjestelmien kyberturvallisuuden testaamista eri tietoturvatoimijoiden puolesta. Sotilasorganisaatiossa aihealue on arka, koska riittävän kattavan penetraatiotestauksen saavuttamiseksi tulisi testaamiseen osallistua laajamittaisesti myös siviilipuolen toimijoita. Vastaajan C mukaan järjestelmää tulisi testata esim. laajoilla ja kattavilla Hackathon-tyyppisillä kampanjoilla, joissa kehitettävän järjestelmän toimintaa vastaan haastetaan (ulkopuolisia) hyökkääjiä. Tätä voisi suorittaa kaikissa kehitysvaiheissa, sekä yksittäisiin elementteihin, että kattavasti suurempiin kokonaisuuksiin kohdistuen. Tietenkin ongelmana on, että siviilitoimijoilla ei ole käytössään resursseja, joita oikeilla hyökkääjillä on. (C)

Vastaaja A mainitsee vastauksessaan haasteen suojata järjestelmän tuottamaa dataa riittävän tehokkaasti. Koko maasta lasketun aineiston tuottama data verkon solmujen sijoitukselle ja niiden tuottamalle suorituskyvylle yhdistettynä alueen operatiiviseen suunnitelmaan olisi korkean tietoturvaluokan materiaalia, joten kokonaisuuden suojaus on mietittävä tarkasti. Myös pienemmät elementit ja niiden tuottama data esim. harjoituksista operaatioalueen suorituskyvystä tulee osata luokitella oikeaan tietoturvaluokkaan. (A)

Vastaaja B ehdottaa tietovuo- ja pakettikaappauksen keskitettyä hallinnointia parhaan mahdollisen havainnointikyvyn saavuttamiseksi. Edellä mainittujen paikallisten tietojen kerääminen ja ajoittainen lähettäminen yhdistettynä jatkuvaan paikalliseen monitorointiin lienee paras vaihtoehto. Aktiivilaitteiden konfiguraation tiivisteiden jakaminen verkossa mahdollistaisi konfiguraatiohallinnan, mikäli ei voida lähettää kokonaisia konfiguraatiotiedostoja tai niiden muutoksia keskitettyyn pisteeseen. (B) Edellä mainittuja toteutusvaihtoehtoja on esitetty kappaleessa 3.3. Aktiivilaitteiden olisi myös kyettävä menemään tilaan, jossa niiden kyky kuunnella verkkoa on poistettu, mutta ne kykenevät silti vastaanottamaan konfiguraatioita. (B)

4.4. Kyselyn toinen kierros

Kyselyn toinen kierros toteutettiin strukturoidusti koostuen erilaisista väittämistä. Väittämät laadittiin kirjallisuusselvityksen ja kyselyn ensimmäisen kierroksen vastausten pohjalta. Kyselyn toinen kierros lähetettiin samalle vastaajajoukolle kuin ensimmäinen kierros. Vastaajia oli seitsemän kappaletta vastausprosentin ollessa 64%, jota voidaan pitää hyvänä. Kyselyn toisen kierroksen väittämät sekä vastausjakaumat on esitelty liitteessä 4.

Tulokset on analysoitu määrällisellä analyysillä deskriptiivisen eli kuvailevan tilastotieteen menetelmin. Määrällisen analyysin parina pidetään laadullista eli kvalitatiivista tutkimusta, jossa pyritään ymmärtämään kohteen laatua, ominaisuuksia ja merkityksiä kokonaisvaltaisesti. Laadullisen ja määrällisen analyysin välistä eroa usein korostetaan, vaikka molempia suuntauksia voidaan käyttää myös samassa tutkimuksessa ja molemmilla voidaan selittää, tosin eri tavoin, samoja tutkimuskohteita. Määrällisellä analyysilla pyritään selvittämään esimerkiksi erilaisia ilmiöiden syy-seuraussuhteita, ilmiöiden välisiä yhteyksiä tai ilmiöiden yleisyyttä ja esiintymistä numeroiden ja tilastojen avulla. Määrällisessä analyysissa on tavanomaista, että tutkimusaineistoa kuvataan tilastollisesti ja havainnollistetaan graafisesti. Tilastollisella analyysilla voidaan todeta aineistosta esimerkiksi ilmiöiden määriä, yleisyyttä, jakautumista ja jäsentymistä luokkiin. [46]

Tilastotiede on yleinen menetelmätiede, jota sovelletaan, jos reaalimaailman ilmiöstä halutaan tehdä johtopäätöksiä ilmiötä kuvaavien kvantitatiivisten tai numeeristen tietojen perusteella sellaisissa tilanteissa, joissa tietoihin liittyy epävarmuutta tai satunnaisuutta. Tilastollisten menetelmien avulla reaalimaailman ilmiöitä kuvaavat numeeriset tai kvantitatiiviset tiedot jalostetaan sellaiseen muotoon, että ilmiöitä koskevat johtopäätökset tulevat mahdollisiksi. Kuvailevan tilastotieteen avulla tutkimuksen kohteena olevasta ilmiöstä kerättyjä numeerisia tai kvantitatiivisia tietoja voidaan kuvailla ja esitellä. Tilastollinen inferenssi eli päättely kehittää ja soveltaa menetelmiä, joiden avulla tutkimuksen kohteena olevasta ilmiöstä voidaan tehdä johtopäätöksiä ilmiöstä kerättyjen kvantitatiivisten tietojen perusteella. [47]

Toisen kyselykierroksen tulokset on esitetty prosenttijakaumina ja analysoinnissa tulokset on jaoteltu edelleen kolmeen kategoriaan: 1. merkittävän konsensuksen saaneet väittämät 2. osittaisen konsensuksen saaneet väittämät ja 3. ei konsensusta saaneet väittämät. Tulosten luokittelussa olisi voitu hyödyntää aritmeettista keskiarvoa, mutta vastaajien lukumäärän ollessa vähäinen, voi yhdelläkin täysin eriävällä näkemyksellä olla merkitystä, mikä hukkuisi aritmeettisen keskiarvon tarkastelussa. Tästä syystä jaottelussa on päädytty prosentuaaliseen jakaumaan, jossa on korostunut neutraalien ja eriävien vastausten suhteellinen osuus.

Mikäli tuloksien vastausvaihtoehdoissa yhteen laskettuna eri mieltä (vastausvaihtoehdot 1 ja 2) tai samaa mieltä (vastausvaihtoehdot 4 ja 5) vastanneiden osuus ylitti 85%, on tulos jaoteltu kategoriaan 1. Mikäli tuloksien vastausvaihtoehdoissa yhteen laskettuna eri mieltä (vastausvaihtoehdot 1 ja 2) tai samaa mieltä (vastausvaihtoehdot 4 ja 5) vastanneiden osuus ylitti 70%, on tulos jaoteltu kategoriaan 2. Mikäli tuloksissa on enemmän hajontaa kuin edellä mainituissa, on tulos jaoteltu kategoriaan 3. Mikäli väittämän kanssa eri mieltä (vastausvaihtoehdot 1 ja 2) vastanneiden tulosten osuus oli yli 50%, on tästä myös erikseen mainittu väittämän oletetun paikkansa pitävyyden suhteen.

4.5. Merkittävän konsensuksen saaneet väittämät

4.5.1 Kognitiivisen tietoliikennejärjestelmän ominaisuudet:

Vastaajat olivat yhtä mieltä tutkimuksessa esitetyistä kognitiivisen radion vähimmäisominaisuuksista: dynaaminen spektrinkäyttö, DSA, yhteyksien adaptiivisuus ja radioresurssien hallinta (RRM) ja itsenäisesti organisoituva verkko (SON). Vastaajien mukaan kognitio tulee myös tuoda mukaan koko verkkoon, jotta radioverkko voi mukautua muuttuvaan ympäristöön.

Kaikki vastaajat olivat sitä mieltä, että kognitiivinen tietoliikennejärjestelmä eroaa ohjelmistoohjatusta tietoliikenneverkosta, koska vaikka SDN voi säätää nopeasti verkon käyttäytymistä, siitä puuttuu kognitio ja tietoisuus ympäristöstä ja siten myöskin tieto siitä, mihin sopeutua. Samoin liki yhtä mieltä oltiin siitä, että kognitiivinen tietoliikennejärjestelmä eroaa myös kognitiivisesta radiosta (CR), koska kognitiivinen radio on tietoinen vain paikallisesta spektriympäristöstä ja siten tarkoitettu optimoimaan vain point-to-point -yhteydet, eikä se voi optimoida kokonaisuutta koko verkon suorituskyvyn suhteen. Samaa mieltä oltiin myös kognitiivisen verkon kolmesta perusominaisuudesta: tilannetietoisuus, oppimis- ja päätöksentekokyky sekä täysin kontrolloitavat tietoliikenneparametrit ja -asetukset, joista voidaan johtaa kognitiiviset perustoiminnot: havainnointi, oppiminen, päätöksenteko, itseohjautuvuus ja automaattinen konfiguroituminen.

Kognitiivisen verkon vaatimasta yhteisestä kontrollikanavasta kuusi seitsemästä oli yhtä mieltä, että se toimii avainelementtinä koko verkon yhteisen ohjaamisen suhteen. Huomioitavaa on kuitenkin, että yksi vastaaja oli täysin eri mieltä. Kaikki vastaajat olivat sitä mieltä, että verkonhallinnan suhteen kognitiivisen tietoliikennejärjestelmän myötä voidaan keskittyä enemmän itse tehtävän suorittamiseen joutumatta toteuttamaan vaikeita verkkomääritystehtäviä operaation aikana. Tästä syystä myös tekninen konfigurointi ennen operaatioita vähenee.

4.5.2 Kognitiiviseen taktiseen tietoliikennejärjestelmään kohdistuvat uhkat

Kaikki vastaajat olivat sitä mieltä, että SDN:n keskitetty ohjaus voi muodostua kriittiseksi uhaksi, koska se hallitsee kaikkia verkon laitteita yhdestä paikasta käsin, mistä syystä sen toimintavarmuus on kriittinen. Kaikki paitsi yksi vastaaja olivat sitä mieltä, että SDN-verkon uhkia ovat muun muassa keskitetyn hallinnan turvallisuuden takaaminen, ohjaimen ja verkkolaitteiden välisen viestinnän turvaaminen ja verkkosovellusten vahingollisen toiminnan estäminen.

Kontrollikanavan suhteen valtaosa oli sitä mieltä, että erillinen kontrollikanava on altis muodostumaan kriittiseksi vikaantumispisteeksi. Myös staattisen kontrollikanavan hyppyparametrien toteutuksen vuotaminen koettiin merkittävänä uhkana.

4.5.3 Kognitiivisen taktisen tietoliikennejärjestelmän kyberturvallisuutta parantavat toteutusvaihtoehdot

Kaikki vastaajat olivat sitä mieltä, että SDN:n hajautettu arkkitehtuuri tulisi ottaa osaksi kognitiivista taktista tietoliikenneverkkoa. Vastaajat olivat myös yhtä mieltä siitä, että ohjelmisto-ohjaus (SDN) yhdessä verkkovirtualisoinnin (NFV) kanssa helpottaa verkkojen dynaamista resurssien hallintaa sekä palvelujen ohjausta, ja että näiden molempien lähestymistapojen yhdistelmällä voidaankin saavuttaa etuja hallinnan ja operoinnin suhteen. Myös kaikki paitsi yksi vastaaja oli sitä mieltä, että ohjelmisto-ohjatun verkon tietoturva on perinteistä tietoverkkoa helpompi pitää ajan tasalla päivittämällä sovelluksia sen sijaan, että vaihdettaisiin fyysisiä verkkolaitteita tai päivitettäisiin niitä yksittäin. Lisäksi arkkitehtuurissa uusien ominaisuuksien toteuttaminen on nopeampaa.

Klusterointi koettiin tärkeäksi robustin verkon suunnittelussa. Vastaajat olivat sitä mieltä, että klusteroinnin tulisi siksi tukea myös muita taktisissa kognitiivisissa radioverkoissa käytettyjä tekniikoita. Vastaajat olivat myös sitä mieltä, että suojautumisen näkökulmasta kognitiivisen verkon tulee varautua erilaisiin tilanteisiin etukäteen simuloimalla ja mallintamalla häirintä- ja häiriöskenaarioiden vaikutuksia kognitiivisen radion eri toimintatapamalleissa.

Kontrolliliikenteen turvaamiseksi tärkeimmäksi ratkaisuksi koettiin hajaspektritekniikoiden hyödyntäminen. Myös dynaaminen kontrollikanavan allokointi nähtiin käyttökelpoisena. Liki kaikkien vastaajien mielestä solmujen luotettavuuden arviointitekniikat tulisi olla kiinteänä osana kognitiivista tietoliikenneverkkoa.

Ensisijaisen käyttäjän emulointihyökkäyksiä varten signaalin aitouden todentamiseksi kaikki olivat todennusprotokollan käyttämisen kannalla. Kaikki olivat myös sitä mieltä, että kontrollikanava tulisi olla kaistan ulkopuolella ja toteuttaa erittäin nopealla kontrolliliikenteen ja hyötyliikenteen välisellä taajuushypinnällä. Kontrollikanavan rakenteen suhteen valtaosa oli sitä mieltä, että kanavan rakenteen tulee olla dynaaminen, muuntuva ja klusteroitu (vaatii enemmän resursseja, mutta on häiriösietoisempi). Kaikki olivat sitä mieltä, että kognitiivisen taktisen tietoliikennejärjestelmän kyberturvallisuutta tulisi testata hyökkäämällä sitä vastaan sekä laajoilla ja kattavilla kampanjoilla yhteistyössä siviilitoimijoiden kanssa (kuten Hackathon, Pentest) että PV:n sisäisellä tunkeutumistestauksella integraatio- ja testausympäristössä (PVITY) osana järjestelmän kehitystä.

4.5.4 Muut vaatimukset

Järjestelmän muiden vaatimusten suhteen valtaosa oli sitä mieltä, että kognitiivisen taktisen tietoliikenneverkon tulisi kyetä automaattisesti suunnittelemaan verkkorakenteensa. Vastaajat olivat myös liki yhtä mieltä siitä, että lopullinen vastuu tulee kuitenkin olla käyttäjällä, ja kognitiivista verkkoa ja sen toimintaa ja toiminnallisuuksia tulee kyetä valvoa ja hallita ihmisen toimesta. Tämä tarkoittaa myös sitä, että kognitiivisessa verkossa tulisi olla mahdollisuus manuaaliohjaukseen protokollien ja yhteydenmuodostuksen saralla, sekä käyttäjän mahdollisuus poistaa yhteyksiä ja toiminnallisuuksia.

Liki kaikki olivat sitä mieltä, että antennien sekä radion olisi kyettävä hyödyntämään mahdollisimman laajaa taajuuskaistaa (UHF, VHF, HF). Tästä laajasta taajuusalueesta johtuen valtaosa oli myös sitä mieltä, että antenneja tulee olla useanlaisia, joista osa olisi suunta-antenneja. Kognitiivisella radiolla tulisi olla myös kyky ohjata radion antenneja. Myös siitä oltiin hyvin samaa mieltä, että älykkäiden SBA-tyyppisten antennien avulla voitaisi parantaa merkittävästi verkon palvelukykyä. Samoin automaattisesti radiosta ohjatut aktiiviantennit voivat optimoida verkkoa radioiden hypintä- ja taajuus-suunnitelman mukaiseksi vähentäen havaittavuutta parhaimmillaan kaksinkertaistaen linkkipituudet.

Valtaosa oli sitä mieltä, että kognitiivisen taktisen verkon tulisi muodostaa havainnoista käyttäjälle helpommin tulkittavissa olevaa dataa visuaalisen käyttöliittymän avulla, jolloin myös käyttäjä pysyy helpommin tilannekuvan tasalla. Kaikki paitsi yksi olivat sitä mieltä, että tekoälylle tulee antaa päätöksentekokyky pieniin parametrien vaihtoon, mutta tekoälyn tulee kyetä myös ennalta esitellä suuremmat optimoinnit ja verkkorakenteen muutokset.

4.6. Osittaisen konsensuksen saaneet väittämät

4.6.1 Kognitiivisen tietoliikennejärjestelmän ominaisuudet

Valtaosa vastaajista oli sitä mieltä, että kognitiivisella radiolla tulee olemaan merkittävä rooli elektronisessa sodankäynnissä. Yksi vastaaja oli hieman eri mieltä roolin merkittävyydestä. Myös verkonlaajuisten konfigurointien ja uusien ominaisuuksien kehittämisen helpottamiseksi koettiin SDN:n tarjoavan ratkaisumallin.

SDN-arkkitehtuuriin liittyen kaksi vastaajaa koki olevansa hieman eri mieltä väittämän kanssa. Tämä oli hieman yllättävää, koska kirjallisuudessa useampi merkittävä lähde tuki väittämää. Viisi vastaajaa oli kuitenkin samaa mieltä väittämän kanssa. Samoin yksi vastaaja oli hieman eri mieltä SDN-verkon kolmesta perusperiaatteesta (fyysisen ja ohjelmistokerroksen erottaminen, loogisesti keskitetty ohjaus ja verkkotoimintojen ohjelmoitavuus). SDN arkkitehtuurin pääkomponenteista; hallintatasolla olevasta ohjaimesta (SDN Controller) sekä liikennetasolla olevasta liikennettä välittävästä laitteesta (SDN Forwarding Element) oltiin suurin piirtein samaa mieltä kahden vastaajan vastatessa neutraalisti.

Järjestelmän määritelmän päästä-päähän -tavoitteen toteuttamiseksi tarvittavat ohjelmoitavat elementit aiheuttivat pientä hajontaa vastaajissa. Valtaosa oli sitä mieltä, että ilman että kaikki elementit (esim. aliverkot, reitittimet, kytkimet, virtuaaliyhteydet, salausjärjestelmät, siirtomediat, rajapinnat tai aaltomuodot) ovat ohjelmistopohjaisesti konfiguroitavissa, järjestelmä voi sisältää kognitiivisia osia (esimerkiksi kognitiivinen radio), mutta järjestelmä ei ole kokonaisuudessaan kognitiivinen tietoliikenneverkko.

4.6.2 Kognitiiviseen taktiseen tietoliikennejärjestelmään kohdistuvat uhkat

DSA-protokollien tai verkon taajuuspäätösprosessin manipuloitavuudesta suurin osa oli sitä mieltä, että se aiheuttaa merkittävän uhkan järjestelmälle. Yksi vastaajista oli neutraali, ja yksi sitä mieltä, että välttämättä uhka ei ole merkittävä. DSA:n mahdollistamasta seurantahäirinnän kyvystä estää palvelut valtaosa oli sitä mieltä, että uhka on merkittävä tai olemassa, kahden vastatessa neutraalisti.

Perinteiset uhkat, kuten ohjelmistollisten parametrien ja algoritmien suunnittelu, tekeminen, käsittely, säilyttäminen ja henkilöriskit koettiin muodostavan uhkan vihollisen tiedustelun suhteen viiden vastaajan toimesta.

4.6.3 Kognitiivisen taktisen tietoliikennejärjestelmän kyberturvallisuutta parantavat toteutusvaihtoehdot

Viisi vastaajaa oli sitä mieltä, että yksittäisen solmun ja verkon tavoitteiden välisten optimointiristiriitojen välttämiseksi tulisi järjestelmässä olla konfliktien purkamisprosessi. Neljä vastaajaa oli sitä mieltä, että kognitiivisen verkon parametreja suunnitellessa tulisi huomioida, miten välttää verkon toiminnan perusteella vihollisen häirinnän tehoamisen paljastuminen.

4.6.4 Muut vaatimukset

Suuri osa oli sitä mieltä, että kognitiivisen verkon adaptiivisuuden ja optimoinnin suhteen tehtävän ja operaation suoritusvaiheen tulisi vaikuttaa haluttuun lopputulokseen (tilannekuva, salaaminen, harhauttaminen, tiedustelu, tulenjohto, häirinnän väistö, kokonaissuorituskyky), samoin kuin siitä, että kognitiivisilla radioilla tulee olla kyky toimia ELSO-sensoreina ja häirintälähettiminä tarvittaessa. Moni piti myös erittäin tärkeänä, että kognitiivisen radioverkon tulisi kyetä toimimaan yllättävästi, esimerkiksi vihollisen käyttämän taajuusalueen hyödyntämisellä. Suuri osa vastasi, että kognitiivisen taktisen verkon tulisi kyetä automaattiseen toimeenpanoon esim. tuottamalla automaattiset asemakäskyt viestiasemille. Moni oli myös sitä mieltä, että verkon muutoksiin liittyen tulisi olla mahdollisuus käyttäjän hyväksynnälle.

4.7. Ei konsensusta saaneet väittämät

4.7.1 Kognitiivisen tietoliikennejärjestelmän ominaisuudet

Kognitiivisen verkon verkonlaajuinen tiedonvaihto (esim. hajautettu taajuushavainnointi) jakoi vastaajien mielipiteitä: neljä vastaajaa oli sitä mieltä, että tieto pitää jakaa verkonlaajuisesti ja päätökset kyetä tekemään hajautetusti, kun taas yksi oli neutraali ja kaksi eri mieltä.

4.7.2 Kognitiiviseen taktiseen tietoliikennejärjestelmään kohdistuvat uhkat

Eniten neutraaleja vastauksia keräsi väite, että hajautettu taajuushavainnointi muodostaa verkossa pullonkaulan vaihtaessaan spektrianturidataa, jolloin se vaatii luotettavat tietoliikenneyhteydet anturipäätelaitteiden ja päätöksiä suorittavan fuusiokeskuksen välillä. Tämä viittaisi siihen, että mielipide on hankala muodostaa sen suhteen, muodostuuko pullonkaulausta merkittävää uhkaa vai ei. Samoin kolme vastasi neutraalisti liittyen mahdolliseen uhkaan DSA:n mahdollistaman kanavanväistön tapahtuessa laumakäyttäytymisellä.

Ensisijaisen käyttäjän emulointihyökkäyksen suhteen enemmistö oli sitä mieltä, että uhka on olemassa tai erittäin merkittävä, kahden ollessa neutraali ja yhden täysin eri mieltä. Avoimen vastausmahdollisuuden perusteella täysin eri mieltä ollut vastaaja perusteli kantansa sillä, että käyttäjä (primääri/sekundääri) pystytään myös tunnistamaan salauksen avulla. Hajautettua taajuushavainnointia (DSS) vastaan kohdistettu taajuushavainnoinnin väärentämishyökkäys koettiin uhkaksi kolmen vastaajan toimesta, kolmen ollessa neutraali ja yhden eri mieltä.

Kontrolliliikennettä vastaan kohdistuvien uhkien suhteen kontrollikanavan tukkeutuminen koettiin erittäin merkittäväksi uhkaksi kolmen vastaajan toimesta. Kolme vastaajaa oli kuitenkin neutraaleja ja yksi vastaaja hieman eri mieltä. Kontrolliliikenteen luottamuksellisuuden ja eheyden suhteen kolme vastaajaa oli sitä mieltä, että ne voivat muodostua uhkaksi koko verkon toiminnalle, mutta kolme vastaajaa oli neutraaleja ja yksi hieman eri mieltä. Uhkaan dynaamisen kontrollikanavan edellyttämän neuvottelun viiveestä kontrollikanavan muodostamiseksi ELSO:n vaikutuksen alla ei otettu kantaa neljän vastaajan toimesta. Kaksi vastaajaa koki sen uhkaksi, yhden ollessa eri mieltä. Myöskään verkon liiallista tukeutumista automatisointiin ei koettu uhkana.

Verkkotopologian klusteroinnin aiheuttaman liiallisen viiveen suhteen suurin osa ei osannut ottaa kantaa (neljä neutraalia vastausta). Kaksi oli sitä mieltä, että viivettä voi tulla, yhden ollessa eri mieltä. Kolme vastaajaa oli eri mieltä siitä, että ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tasot ovat alttiita palveluksenestohyökkäyksille ja muodostavat siten houkuttelevan kohteen. Kaksi vastaajaa oli neutraaleja ja kaksi vastaajaa koki palveluksenestohyökkäykset uhkana. Tekoälyn tuottaman aineiston niin järjestelmästä kuin ympäristöstä, ja siihen liittyvät tietoturvaluokittelut ja tiedon säilyttäminen ja käyttö ei nähty aiheuttavan uhkaa.

4.7.3 Kognitiivisen taktisen tietoliikennejärjestelmän kyberturvallisuutta parantavat toteutusvaihtoehdot

SDN-verkkojen mahdollistamaa reitityssääntöjen asentamista kytkimiin tarvittaessa (reaktiivisesti), ja täten reaktiivisen vuosääntöjen luomisen hyödyntämistä esim. palvelunestohyökkäyksissä koettiin erittäin merkittäväksi turvallisuutta parantavaksi toteutusvaihtoehdoksi kolmen vastaajan toimesta, mutta kaksi vastaajaa koki tämän neutraaliksi ja yksi ei niin merkittäväksi. Myöskään ohjaimen mahdollisen ylikuormittumisen välttäminen ohjaimen hajauttamisella ei koettu merkittäväksi ratkaisuksi kuin neljän vastaajan toimesta. Ohjaimen vuomerkintöjen väliaikainen tallennus ja vuosääntöjen vaihtaminen tai poistaminen kytkimistä tarpeen mukaan koettiin neljän vastaajan toimesta tärkeäksi, kahden vastaajan ollessa kuitenkin eri mieltä. Palvelunestoliikenteen dynaaminen ohjaus esimerkiksi niin sanottuun hunajapurkkiin hyökkäyksen analysoimiseksi koettiin merkittäväksi keinoksi neljän vastaajan toimesta, kahden ollessa neutraali ja yhden hieman eri mieltä.

Neljä vastaajaa oli sitä mieltä, että Ethanen tietoturvan toteutuksesta voitaisiin ottaa oppia ohjelmisto-ohjattuihin tietoverkkoarkkitehtuureihin. Kaksi ei ottanut siihen kantaa ja yksi oli hieman eri mieltä. Ohjelmisto-ohjatun tietoturvallisuuden (SDSec, Software-Defined Security) kognitiivisen tietoliikenneverkon turvallisuuden parantamisesta erityisesti pääsynhallinnan ja autentikoinnin suhteen oltiin hieman epävarmoja, kolmen vastatessa neutraalisti.

Kontrollikanavan liikenteen mukautettavuus sen hetkiseen liikennemäärään nähtiin merkittäväksi vain kolmen vastaajan toimesta. Häirinnän väistötoimenpiteenä kontrollikanavalla CDMA-koodijakokanavoinnin käyttöä ennalta määriteltyjen jakokoodien kanssa ei koettu merkittäväksi toteutusvaihtoehdoksi. Myöskään kahden radioetupään hyödyntämistä kontrolliliikenteeseen ei koettu merkittäväksi.

Etäisyyssuhteen (DRT) hyödyntäminen ensisijaisen käyttäjän tunnistamisessa ei koettu toteutuskelpoiseksi taktisessa verkossa suurimman osan vastaajien toimesta. Myöskään etäisyyserotestiä (DDT, distance difference test) ei nähty toteutuskelpoiseksi.

4.7.4 Muut vaatimukset

Vastaajat jakautuivat sen suhteen, tulisiko kognitiivisen taktisen verkon suunnitteluperusteita luoda edelleen manuaalisesti. Vastaajat eivät olleet varmoja myöskään siitä, tulisiko tekoälyn tekemät päätökset tarkastaa järjestelmän ohjaus- ja suunnitteluhenkilöstön toimenpitein.

Vastaukset jakautuivat myös sen suhteen, tulisiko kognitiivisilla radioilla tulee olla kyky häirintälähettimenä toimiessaan lähettää viholliselle autenttisen oloista liikennettä. Myös kognitiiviseen radioverkon liitettävyys vanhemman sukupolven ohjelmistoradioiden suhteen jakoi vastaajat samaa mieltä ja eri mieltä oleviin.

Tekoälyavusteista verkon hallintasovellusta (esim. tekoälyavusteinen Network Manager), joka voisi suunnitella verkon rakenteen vastaamaan haluttua verkon suorituskykyä, kieltää huonot naapuruudet ja poistaa tarpeettomat yhteydet, ei koettu yhteisesti tärkeäksi vaatimukseksi. Myöskin rajapinta mahdollisen johtamis- ja tilannekuvajärjestelmän (esim. MATI) kanssa jakoi mielipiteitä.

5. JOHTOPÄÄTÖKSET

5.1. Johtopäätökset

5.1.1 Kognitiivinen radio ja kognitiivinen taktinen tietoliikennejärjestelmä

Jotta radio on kognitiivinen, tulee siitä löytyä seuraavat vähimmäisominaisuudet: dynaaminen spektrinkäyttö, DSA, yhteyksien adaptiivisuus ja radioresurssien hallinta (RRM) ja itsenäisesti organisoituva verkko (SON). Kognitiivinen radio on kognitiivisen taktisen tietoliikennejärjestelmän solmun tärkeä osa, mutta se on tarkoitettu optimoimaan vain point-to-point -yhteydet, eikä se voi optimoida kokonaisuutta koko verkon suorituskyvyn suhteen.

Jotta koko tietoliikennejärjestelmä olisi kognitiivinen, päästä-päähän -tavoitteen toteuttamiseksi tarvitaan ohjelmistopohjaisesti ohjelmoitavia elementtejä kaikissa kerroksissa (esim. aliverkot, reitittimet, kytkimet, virtuaaliyhteydet, salausjärjestelmät, siirtomediat, rajapinnat ja aaltomuodot). Ilman ohjelmistopohjaisesti konfiguroitavia elementtejä järjestelmä voi sisältää kognitiivisia osia (esimerkiksi kognitiivinen radio), mutta järjestelmä ei ole kokonaisuudessaan kognitiivinen tietoliikennejärjestelmä, eikä siitä saada kaikkea hyötyä irti. Kognitiivisella tietoliikennejärjestelmällä on kolme perusominaisuutta: tilannetietoisuus, oppimis- ja päätöksentekokyky sekä täysin ohjelmoitavat tietoliikenneparametrit ja -asetukset, joista voidaan johtaa kognitiiviset perustoiminnot: havainnointi, oppiminen, päätöksenteko, itseohjautuvuus ja automaattinen konfiguroituminen. Tällä hetkellä vaikuttaa siltä, että ohjelmisto-ohjattu arkkitehtuuri (SDN) on lupaavimpia toteutusvaihtoehtoja kognitiiviselle tietoliikennejärjestelmälle.

Kognitiivisen radion sekä antennien olisi kyettävä hyödyntämään mahdollisimman laajaa taajuuskaistaa (UHF, VHF, HF). Tästä laajasta taajuusalueesta johtuen antenneja tulee olla useanlaisia, joista osa on suunta-antenneja. Kognitiivisella radiolla tulisi siksi olla myös kyky ohjata radion antenneja. Tästä syystä jo olemassa olevien älykkäiden SBA-tyyppisten antennien hyödyntämisellä voitaisiin parantaa merkittävästi verkon palvelukykyä. Samoin automaattisesti radiosta ohjatut aktiiviantennit voisivat optimoida verkkoa radioiden hypintä- ja taajuus-suunnitelman mukaiseksi vähentäen sähkömagneettisen säteilyn havaittavuutta viholliselle samalla parhaimmillaan kaksinkertaistaen linkkipituudet.

Kognitiivinen radio tulee muuttamaan elektronisen sodankäynnin luonnetta. Suurin osa asiantuntijoista oli sitä mieltä, että kognitiivisilla radioilla tulee olla kyky toimia ELSO-sensoreina ja häirintälähettiminä tarvittaessa. Suuri osa piti myös erittäin tärkeänä, että kognitiivisen radioverkon tulisi kyetä toimimaan yllättävästi, esimerkiksi vihollisen käyttämän taajuusalueen hyödyntämisellä. Edellä mainituista suorituskyvyistä johtuen luultavasti myös perinteisiin viestiasemiin tultaisiin yhdistämään niin ELTI- kuin ELVA-kykyjä. ELSO:n kilpavarustelu tulee todennäköisesti keskittymään enemmän ELVA:n älykkyyteen, jotta kognitiivista järjestelmää vastaan kohdistuva vaikutus voidaan hyödyntää tehokkaimmalla mahdollisella tavalla. Tärkein painopiste tulee olemaan taajuushavainnoinnin ja taajuuspäätösprosessin kokonaisvaltaisessa häirinnässä. Myös kontrolliliikenne muodostaa houkuttelevan kohteen ELVA:lle.

Yleisen operoinnin ja verkonhallinnan suhteen kognitiivisen tietoliikennejärjestelmän hyötyjen myötä voidaan keskittyä enemmän itse tehtävän suorittamiseen joutumatta toteuttamaan vaikeita verkkomääritystehtäviä operaation aikana. Tästä syystä myös tekninen konfigurointi ennen operaatioita vähenee.

Tämän tutkimuksen perusteella jäi ristiriitaiseksi, tulisiko kognitiivisen taktisen tietoliikennejärjestelmän käyttää koko verkonlaajuista tiedonvaihtoa, johon esimerkiksi jaettu taajuushavainnointi kuuluu. Kirjallisuuden perusteella jaettu taajuushavainnointi voi merkittävästi parantaa järjestelmän toimintaa, mutta asiantuntijakyselyn perusteella asia ei vaikuta yksiselitteiseltä. Tähän saattaa osittain liittyä vastauksissa korostunut suositus verkon klusteroinnille, mikä saattaa selittää mielipiteen koskien verkonlaajuista tiedonvaihtoa. Jos kysymys olisi muotoiltu käsittämään jokaisen klusterin sisällä tapahtuvaa tiedonvaihtoa ja taajuushavainnointia, tulos olisi voinut olla eri.

5.1.2 Kognitiivista taktista tietoliikennejärjestelmää vastaan kohdistuvat kyberuhkat

Koska kognitiivinen tietoliikennejärjestelmä sisältäisi merkittävästi nykyisiä järjestelmiä enemmän ohjelmistollisia parametreja ja algoritmeja, perinteiset uhkat, kuten näiden parametrien ja algoritmien suunnittelu, tekeminen, käsittely, säilyttäminen ja henkilöriskit muodostavat uhkan vihollisen tiedustelun suhteen. Nämä uhkat liittyvät erityisesti korkean tietoturvaluokan teknisten hankkeiden koko elinkaareen.

Sekä kirjallisuuden että asiantuntijakyselyn perusteella SDN:n keskitetty ohjaus voi muodostua kriittiseksi uhaksi, koska se hallitsee kaikkia verkon laitteita yhdestä paikasta käsin, ja sen toimintavarmuus on siten kriittinen. SDN-arkkitehtuurin uhkia ovat muun muassa keskitetyn hallinnan turvallisuuden takaaminen, ohjaimen ja verkkolaitteiden välisen viestinnän turvaaminen ja verkkosovellusten vahingollisen toiminnan estäminen. Sen sijaan palvelunestohyökkäyksiä SDN-verkoissa ei koettu asiantuntijoiden toimesta niin merkittävänä uhkana sotilaallisessa kontekstissa, kuin mitä kirjallisuusselvityksen perusteella olisi voinut kuvitella.

Kognitiivinen taktinen radioverkko tarvitsee kontrolliliikennettä varten kontrollikanavaratkaisuja. Kontrollikanavan suhteen voidaan tehdä johtopäätös, että erillinen kontrollikanava on altis muodostumaan kriittiseksi vikaantumispisteeksi. Kanavan sisäinen kontrollikanava vaatii tehokasta taajuushypytystä, ja kontrollikanavan hyppyparametrien toteutuksen vuotaminen tai sen murtaminen vihollisen toimesta on myös merkittävä uhka erityisesti verkonlaajuisen staattisen kontrollikanavan tapauksessa. Sen sijaan tutkimuksessa esiintyi ristiriitaa sen suhteen, muodostaako kontrolliliikenteen tukkeutuminen, luottamuksellisuus ja eheys tai dynaamisen kontrollikanavan muodostumisen viive merkittävää uhkaa järjestelmälle. Kolme asiantuntijaa olivat sitä mieltä, että edellä mainitut voivat muodostaa merkittävän uhkan, mutta kolmen neutraalin ja yhden hieman eri mieltä olevan vastauksen perusteella johtopäätöksen tekeminen ei ole varmaa.

Kontrolliliikenteen lisäksi DSA-protokollien tai verkon taajuuspäätösprosessin manipuloitavuus kyber/EW-vaikuttamisella muodostaa myös merkittävän uhkan. DSA voi mahdollistaa seurantahäirinnän, jonka vaikutus verkonlaajuisesti voi olla merkittävä.

Ensisijaisen käyttäjän emulointihyökkäystä ei pidetty merkittävänä uhkana asiantuntijoiden toimesta. Tässä näkyy todennäköisesti se, että siviilimaailmassa ei useinkaan turvauduta niin järeisiin todennus- ja salausprotokolliin kuin asevoimien järjestelmissä. Riittävän vahvat todennus- ja salausprotokollat ovat tärkeässä roolissa emulointihyökkäyksen estämiseksi.

5.1.3 Kognitiivisen taktisen tietoliikennejärjestelmän kyberturvallisuutta parantavat toteutusvaihtoehdot ja vaatimukset

Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin suomista kyberturvallisuutta parantavista mahdollisuuksista muodostui hieman ristiriitainen tulos. Moni asiantuntija oli neutraali sen suhteen, että SDN-arkkitehtuurin suomista mahdollisuuksista muun muassa reaktiivinen reititys-sääntöjen asentaminen kytkimiin, vuosääntöjen poistaminen tai muokkaaminen tai liikenteen ohjaaminen hunajapurkkiin hyökkäyksen analysoimiseksi toisi merkittävää parannusta järjestelmän kyberturvallisuudelle. Toki edellä mainitut tulokset voivat osaltaan liittyä myös siihen, että vastaajat eivät kokeneet palvelunestohyökkäyksiä kovin merkittäväksi uhkaksi taktisissa kognitiivisissa tietoliikennejärjestelmissä. Yksi mahdollisuus SDN:n tietoturva-arkkitehtuurille olisi ottaa mallia Ethanen tietoturvan toteutuksesta. Toisaalta sen suhteen ei oltu täysin yksimielisiä asiantuntijoiden suhteen.

Tutkimuksen perusteella SDN:n hajautettu arkkitehtuuri tulisi ottaa osaksi kognitiivista taktista tietoliikenneverkkoa, koska SDN:n ohjaimen sijoittaminen yhteen paikkaan muodostuisi kriittiseksi uhkaksi. Asiantuntijat olivat myös yhtä mieltä siitä, että ohjelmisto-ohjaus (SDN) yhdessä verkkovirtualisoinnin (NFV) kanssa helpottaa verkkojen dynaamista resurssien hallintaa sekä palvelujen ohjausta, ja että näiden molempien lähestymistapojen yhdistelmällä voidaankin saavuttaa etuja hallinnan ja operoinnin suhteen. Ohjelmisto-ohjatun verkon tietoturva on myös perinteistä tietoverkkoa helpompi pitää ajan tasalla päivittämällä sovelluksia sen sijaan, että vaihdettaisiin fyysisiä verkkolaitteita tai päivitettäisiin niitä yksittäin, ja lisäksi arkkitehtuurissa uusien ominaisuuksien toteuttaminen on nopeampaa.

Tutkimuksen perusteella taktisen tietoliikennejärjestelmän klusterointi on tärkeää robustin verkon suunnittelussa. Klusteroinnin tulisi siksi tukea myös muita taktisissa kognitiivisissa radioverkoissa käytettyjä tekniikoita. Yksi tällainen verkon klusterointia tukeva tekniikka on dynaaminen kontrollikanava. Valtaosa asiantuntijoista suosittelisikin staattisen koko verkon laajuisen kontrollikanavan sijaan dynaamista muuntuvaa kontrollikanavarakennetta, vaikka se vaatiikin enemmän resursseja ja syö hyötyliikenteeltä suorituskykyä. Dynaaminen kontrollikanava on kuitenkin häiriösietoisempi, ja mahdollinen häiriötilanne ei kaada koko verkon toimintaa. Kontrolliliikenteen turvaamiseksi tärkeimmäksi ratkaisuksi koettiin hajaspektritekniikoiden hyödyntäminen. Käytännössä tämä tarkoittaa, että kontrollikanavan tulisi olla kaistan ulkopuolella ja toteuttaa erittäin nopealla kontrolliliikenteen ja hyötyliikenteen välisellä taajuushypinnällä. Erittäin häiriösietoisia hajaspektritekniikoita käytettäessä on kuitenkin huomioitava sen alentavan tiedonsiirtokapasiteettia huomattavasti.

Bysanttilais- ja taajuushavainnoinnin väärentämishyökkäysten varalle haitallisten toisiokäyttäjien tunnistamiseksi ja eristämiseksi muusta verkosta tulisi käyttää luotettavuuden arviointia kognitiivisissa tietoliikennejärjestelmissä. Luotettavuuden arvioinnin tehtävänä osana tunkeutumisen havainnointia on paljastaa toisiokäyttäjät, jotka tuottavat valheellista informaatiota järjestelmään. Solmujen luotettavuuden arviointitekniikat tulisi siksi olla kiinteä osa kognitiivista tietoliikennejärjestelmää. Yksi varteenotettava, jo käytännössä testattu tekniikka voi olla tutkimuksessa esitetty TUBE - luottamuspohjainen tilannevaroitusjärjestelmä.

Asiantuntijat olivat yhtä mieltä siitä, että suojautumisen näkökulmasta kognitiivisen tietoliikennejärjestelmän tulee varautua erilaisiin tilanteisiin etukäteen simuloimalla ja mallintamalla häirintä- ja häiriöskenaarioiden vaikutuksia kognitiivisen radion eri toimintatapamalleissa. Samoin järjestelmän kyberturvallisuutta tulisi testata hyökkäämällä sitä vastaan sekä laajoilla ja kattavilla kampanjoilla yhteistyössä siviilitoimijoiden kanssa (kuten mm. hackathon, pentest) sekä PV:n sisäisellä tunkeutumistestauksella integraatio- ja testausympäristössä (PVITY) osana järjestelmän kehitystä.

5.1.4 Kognitiivisen taktisen tietoliikennejärjestelmän muut vaatimukset

Jotta järjestelmän automaatiosta saadaan täydet hyödyt irti operaatioiden suunnittelun ja toimeenpanon suhteen, konsensus oli, että kognitiivisen taktisen tietoliikenneverkon tulisi kyetä automaattisesti suunnittelemaan verkkorakenteensa. Operatiivista käyttöä ajatellen automaattista suunnittelua tulisi täydentää myös automaattisella toimeenpanolla esimerkiksi tuottamalla automaattiset asemakäskyt viestiasemille. Ihmisen tulisi kuitenkin kyetä asettamaan reunaehtoja suunnittelulle, koska kognitiivisen tietoliikennejärjestelmän adaptiivisuuden ja optimoinnin suhteen tehtävän ja operaation suoritusvaiheen tulisi vaikuttaa haluttuun lopputulokseen (esimerkiksi tilannekuvan, salaamisen, harhauttamisen, tiedustelun, tulenjohdon, häirinnän väistön, kokonaissuorituskyvyn suhteen). Kognitiivista tietoliikennejärjestelmää ja sen toimintaa ja toiminnallisuuksia tulee siksi kyetä myös valvomaan ja hallitsemaan ihmisen toimesta. Yhtä mieltä oltiin siitä, että järjestelmässä tulisi olla mahdollisuus myös manuaaliohjaukseen protokollien ja yhteydenmuodostuksen saralla, sekä käyttäjän mahdollisuus poistaa yhteyksiä ja toiminnallisuuksia. Tästä syystä kognitiivisen taktisen tietoliikennejärjestelmän tulisi muodostaa havainnoista käyttäjälle helpommin tulkittavissa olevaa dataa visuaalisen käyttöliittymän avulla, jolloin myös käyttäjä pysyy helpommin tilannekuvan tasalla. Asiantuntijat olivat sitä mieltä, että tekoälylle tulee antaa päätöksentekokyky parametrien vaihtoon, mutta tekoälyn tulee kyetä myös ennalta esitellä suuremmat optimoinnit ja verkkorakenteen muutokset. Suurempiin verkon muutoksiin liittyen tulisi olla mahdollisuus käyttäjän hyväksynnälle.

Kognitiiviseen tietoliikennejärjestelmään voi olla mahdollista liittää vanhemman sukupolven ei-kognitiivisia ohjelmistoradioita, joille kognitio voi antaa rajattuja ohjauskomentoja ja asettaa rajoitetusti tiedonsiirtoparametreja. Tämän suhteen asiantuntijoilla oli erimielisyyttä, tulisiko tätä mahdollisuutta hyödyntää. Samoin se, tulisiko kognitiivisella tietoliikennejärjestelmällä olla rajapinta muiden johtamissovellusten, kuten esimerkiksi MATI2 kanssa, jakoi mielipiteitä. Tekoälyavusteista verkon hallintasovellusta (esim. tekoälyavusteinen Network Manager), joka voisi suunnitella verkon rakenteen vastaamaan haluttua verkon suorituskykyä, kieltää huonot naapuruudet ja poistaa tarpeettomat yhteydet, ei koettu yhteisesti tärkeäksi vaatimukseksi.

5.2. Tutkimuksen kriittinen tarkastelu ja jatkotutkimustarpeet

Tulevaisuudentutkimuksen tieteellisyyttä voi arvioida esimerkiksi Peircen kriteerien näkökulmasta. Peircen mukaan mikä tahansa toiminta on tieteellistä, jos se mukailee viittä eri kriteeriä: kriittisyys, objektiivisuus, itsensä korjaavuus, julkisuus ja toistettavuus [48]. Tulevaisuudentutkimuksen osalta erityisesti väitteiden itsensä korjaavuus ei useinkaan toteudu kuin määrittelemättömän ajanjakson kuluttua. Tieteellisten väittämien tulisi siis periaatteessa olla kumottavissa, mutta ilman tulevaisuudentutkimuksista käytännössä aina puuttuvaa empiiristä tutkimusta se on usein mahdotonta. Monesti tulevaisuudentutkimuksissa ja tässäkin tutkimuksessa käytetyssä delfoi-tutkimusmenetelmässä yhdistetään niin laadullisia kuin kvantitatiivisia menetelmiä, joista laadullisia menetelmiä vaivaa yksiselitteisten luotettavuusmittareiden puute. Tulevaisuuden tutkimiseen liittyy parhaimmillaankin aina paljon epävarmuuksia. Siksi tulevaisuudentutkimuksessa tutkimustuloksiin liittyvä epävarmuus tulee osata suhteuttaa tutkimustuloksiin oikein.

Tutkimuksen analyysin osalta tutkimuksen luotettavuutta heikentää erityisesti tulevaisuudentutkimusta heikentävä itsenäinen työskentelymetodi. Itsenäisessä työskentelyssä on riskinä, että näkemyksistä muodostuu liian subjektiivisia. Tavallisesti erilaisten teknologiavaihtoehtojen ja niiden seurannaisvaikutusten laadintaan varten osoitetaan useita asiantuntijoita, joista muodostetaan työryhmiä. Delfoi-menetelmän käyttöä perustellaan usein sillä, että resurssien takia asiantuntijoiden saaminen saman pöydän ääreen voi olla hyvin haasteellista. Kuitenkin vapaa vuorovaikutus ja keskustelu todennäköisesti vähentäisi väärinkäsityksiä sekä saisi aikaan monipuolisempia ja useita eri näkökulmia yhdistäviä lopputuloksia.

Tutkimuksen reliaabeliudella tarkoitetaan tutkimuksen toistettavuutta, eli kykyä tuottaa eisattumanvaraisia tuloksia [5, s. 216]. Tutkimuksessa käytetty perusjoukko oli varsin pieni, joka vähentää tutkimuksen toistettavuutta. Ainoa henkilöstöryhmä, joka oli varsin hyvin edustettuna perusjoukossa, oli Puolustusvoimien aihealueen asiantuntijat, koska heidän kokonaismääränsä on hyvin vähäinen teollisuuteen tai tiedeyhteisöön verrattaessa. Osittain tämä palvelee kuitenkin tutkimuksen viitekehystä korostamalla tutkimusongelman tarkastelua sotilaallisesta kontekstista.

Pienestä perusjoukosta johtuen kuitenkin jo yhden vastaajan poikkeava vastaskäyttäytyminen on saattanut vaikuttaa merkittävästi yksittäisen mitatun kokonaisuuden merkitykseen ja sitä kautta arvioituun kokonaisuuden tärkeyteen järjestelmän kannalta. Tämä saattoi olla myös syy siihen, miksi avointen vastausten sisällön erittelyllä saadut tulokset poikkesivat osittain merkittävästi monivalinkysymysten tuloksista. Jos monivalintakysymysten vastausvaihtoehdoista olisi poistettu neutraali valinta ”3”, on mahdollista, että useampien kokonaisuuksien välille olisi kyetty saamaan selkeämpiä eroja, sillä osassa kysymyksiä neutraalien vastausten määrä oli huomattava.

Tutkimuksen validiudella tarkoitetaan käytettyjen mittarien tai tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoitus mitata [5, s. 216]. Tämän suhteen tutkimuksen tutkimusongelma sisältää itsessään hyvin laajoja ja monimutkaisia kokonaisuuksia, mistä syystä oli vaikea määritellä täysin yksiselitteisesti ymmärrettäviä kysymyksiä. Osin tästä syystä mittarit ja menetelmät eivät välttämättä vastaa täysin sitä todellisuutta, jota tutkija kuvittelee tutkivansa [5, s. 216]. Tämä voi esiintyä siten, että kyselylomakkeiden kyselyyn saadaan vastaukset, mutta vastaajat ovat voineet käsittää osan kysymyksistä toisin kuin tutkija on alun perin ajatellut [5, s. 216-217]. Koska tässä tutkimuksessa perusjoukko oli pienehkö, on todennäköistä, että jonkinlaista mittausvirhettä on voinut syntyä kysymysten erilaisen käsittämisen takia.

Edellä mainituistakin syistä johtuen tutkimuksessa on alun perin päätytty käyttämään menetelmätriangulaatiota [5, s 218]. Menetelmää hyödyntämällä analyysissä on korostettu kirjallisuusselvityksen ja delfoi-kyselyn suhteen nousseita ristiriitoja. Nousseiden ristiriitojen tarkemmaksi analysoimiseksi olisi pitänyt lähettää vielä kolmas kyselykierros, jossa olisi keskitytty eriävän kannan perustelemiseen. Näin tutkimuksen validiutta olisi saatu parannettua.

Tutkimuksen sisäisen validiteetin tarkastelussa pohditaan aiheutuvatko empiirisen tutkimuksen koetilanteessa saadut tulokset tai muuttujien väliset erot niistä tekijöistä, joiden oletetaan niihin vaikuttavan [49]. Tämän tutkimuksen sisäisen validiteetin arvioinnissa aika näyttelee merkittävintä roolia alati kehityksessä olevan tutkimusaiheen suhteen. Koska teknologia on jatkuvassa kehityksessä, niin kirjallisuudessa olevan tiedon vanheneminen kuin myös asiantuntijoiden tiedon kehittyminen ja oppiminen ovat jatkuvassa muutoksessa. Tämä tutkimus onkin kartoittanut tämänhetkistä tilannetta tutkimusaiheesta. Tietyn ajan kuluttua ja uusien tutkimusten myötä osa esitetyistä asioista voi olla muuttunut, tai asiantuntijoiden käsitykset ja mielipiteet vaihtuneet. Mittaustapahtumassa arvioitsijoiden ja havaintojen tekijöiden näkemyksissä voi tapahtua muutoksia, kun kognitiiviteknologian maturiteetti ja käytettävyys lähestyvät käytännön sovellettavuutta.

Tutkimuksen ulkoista validiteettia arvioidessa pohditaan kvantitatiivisen tutkimuksen tulosten yleistettävyyttä, eli sitä missä populaatiossa, missä tilanteissa, missä asetelmissa saatu tulos voidaan yleistää [49]. Tämän tutkimuksen ulkoista validiteettia parantaa muun muassa se, että asiantuntijoiden vastauksia saatiin eri tahojen edustajilta, niin Puolustusvoimien sisältä kuin ulkopuolelta tiede- ja teknologiayhteisöstä. Perusjoukon ollessa pieni, tutkittavat edustavat kuitenkin vain jotakin osaa kokonaisjoukosta, eikä tulokset ole yleistettävissä vastaamaan kaikkien asiantuntijoiden näkemystä. Tutkimuksen tulosten analysoinnissa olisi ollut mielenkiintoista tarkastella eri henkilöstöryhmien vastausten eroavaisuutta. Tämä olisi tarvinnut kuitenkin suuremman perusjoukon. Vastausten analyysissä teollisuuden, tiedeyhteisön ja Puolustusvoimien välillä olisi ollut mahdollisuus löytää mielenkiintoisia syy-seuraussuhteita.

Aineisto- eli sisältövaliditeetti tarkoittaa tutkimusaineistoon liittyvää validiteettia ja kuvastaa sitä, kuinka hyvin aineiston analysointimenetelmä vastaa tutkimusaineistoa. Sisältövaliditeetti kuvastaa sitä, kuinka hyvin koottu aineisto vastaa ulkopuolisia kriteereitä. [49] Tutkimusaiheeseen liittyvän teoriaosion asiasisällön ja luotettavuuden katsotaan olevan enimmäkseen riippuvainen käytetystä lähdemateriaalista, eli aineiston määrästä ja laadusta, sekä tutkijan kyvystä määrittää, mitkä asiakokonaisuudet liittyvät tutkittavaan aihealueeseen. Koska tutkimuksen viitekehys liittyy sotilaalliseen toimintaan, tutkimuksen sisältövaliditeetin suhteen on pyritty noudattamaan erityisesti sotilaallisesta perspektiivistä tehtyjä tuoreita lähteitä tutkimuksen teorian primäärilähteinä, ja myös muiden lähteiden suhteen keskittymään tiedon vanhenemisesta johtuen tuoreimpiin julkaisuihin. Yhden haasteen tutkimuksessa muodosti siviilitekniikan lähtökohdista muodostuvien tulosten yleistettävyys sotilaskontekstiin. Mahdollisten ristiriitojen selvittämiseksi ja siviililähteiden tuottamien tulosten luotettavuuden parantamiseksi perusjoukon painopisteen muodostivat Puolustusvoimien asiantuntijat.

Tämä tutkimus tarjoaa ensimmäisen suomenkielisen kartoituksen aihealueeseen liittyen. Aihealueen materiaalia on hyvin vähän saatavissa suomeksi, mikä korostaa tämän tutkimuksen tarpeellisuutta. Tutkimuksen tuloksia voitaneen soveltaa esimerkiksi osana suorituskykyjen kehittämistä, olkoonkin että esitetyt tulokset ovat vielä vailla käytännön sovellutuksia. Yksityiskohtaisemmat tulokset olisivat vaatineet tarkempaa rajausta, mikä olisi kuitenkin tässä vaiheessa ollut vaikeaa, sillä pelkästään koko kognitiivisen tietoliikennejärjestelmän käsite näyttäytyi jo alustavan aineistonkeruun yhteydessä vielä suhteellisen epäselvältä.

Mahdollisia jatkotutkimustarpeita ajatellen, kun kognitiiviteknologian maturiteetti ja käytettävyys lähestyvät käytännön sovelluksia kohti kognitiivisia taktisia tietoliikennejärjestelmiä, tulisi koko tietoliikennejärjestelmää ja sen seurannaisvaikutuksia tarkastella esimerkiksi DOTMLPFIi-tarkastelumetodilla [50]. Tätä tutkimusta tehdessä yhtenä haasteena, ja tutkimuksen kokonaisuutta paisuttavana tekijänä oli se, että *kognitiivisen taktisen tietoliikennejärjestelmän* käsitettä ja sen olemusta kartoittavia yleisluontoisia tutkimuksia ei ole toteutettu Suomessa.

Tämän tutkimuksen pohjalta voi todeta, että tutkimusongelman tarkempi rajaaminen olisi jatkotutkimuksissa hyödyllistä yksityiskohtaisempien tulosten saavuttamiseksi. Tutkimusongelma voitaisiin rajata käsittelemään esimerkiksi pelkästään kognitiivisen tietoliikennejärjestelmän taajuushavainnoinnin ja tiedonvaihdon toimintaa, kontrollikanavan toteutusvaihtoehtoja tai solmujen luotettavuuden arviointiin perustuvia tekniikoita. Yksi aktiivinen tutkimusalue NATO:n tiedeyhteisössä on kogniitivinen elektroninen sodankäynti (*cognitive EW*). Jatkotutkimusaiheeksi voisi rajata myös pelkästään kognitiivisuuden tuomat muutokset elektronisessa sodankäynnissä.

LÄHTEET

[1] STO-TR-IST-140 AC/323(IST-140)TP/874. *Cognitive Radio Networks: Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management*. Stotechnical report. Neuilly-sur-Seine, France: North Atlantic Treaty Organization: Science and Technology Organization. 146 p. ISBN 978-92-837-2198-7.

[2] Ahmad, I. *Improving Software Defined Cognitive and Secure Networking*. Doctoral thesis. Oulu, 2018. University of Oulu: Faculty of information technology and electrical engineering: Centre for wireless communications. 80 p. ISBN 978-952-62-1951-6.

[3] Kärkkäinen, A. *Kognitiiviset tietoliikenneverkot verkostopuolustuksessa*. EUK-tutkielma. Helsinki, 2011. Maanpuolustuskorkeakoulu, Esiupseerikurssi, 50 s.

[4] Kosola, J. *Disruptiiviset teknologiat puolustuskontekstissa*. Helsinki: Puolustusvoimat, Materiaaliosasto, 2013. ISBN 978-951-25-2519-5.

[5] Hirsjärvi, S., Remes, P. & Sajavaara, P. *Tutki ja kirjoita*. 21. painos. Helsinki: Kirjayhtymä Oy, 2016. 464 s. ISBN 978-951-31-4836-2.

[6] Tuomi, J, Sarajärvi, A. *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi, 2018. 204 s. ISBN 978-951-319-953-1.

[7] Alasuutari, P. *Laadullinen tutkimus 2.0*. 5. painos. Tampere: Vastapaino, 2011. 331 s. ISBN 978-951-768-385-2.

[8] Marjamäki, M. *Kognitiivinen radio: Vapaat taajuusspektrialueet nyt ja tulevaisuudessa*. Opinnäytetyö. Lahti, 2012. Lahden ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 37 s.

[9] Honko, J. *Kognitiivinen radio sotilaallisen maanpuolustuksen kontekstissa*. Diplomityö. Helsinki, 2015. Maanpuolustuskorkeakoulu, Yleisesiupseerikurssi. 107 s.

[10] Chen, R., Park, J., Hou, Y. & Reed, J. *Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks*. IEEE Communications Magazine, 2008. Vol. 46 (4), p. 50-55. ISSN 1941-0476.

[11] Matinmikko, M. *Spectrum sharing using cognitive radio system capabilities: Methods to obtain and exploit knowledge of spectrum availability*. Doctoral thesis. Oulu, 2012. University of Oulu: VTT Technical Research Centre of Finland. 77 p. ISBN 978-951-38-7943-3.

[12] Mitola, J. *Cognitive radio model-based competence for software radios.* Licence thesis. Stockholm: Royal Institute of Technology, 1999. 146 p. ISSN 1403-5286.

[13] *Cognitive Radio Definitions and Nomenclature*. Software Defined Radio Forum, 2008. 34 p. [viitattu 10.1.2020]. Saatavissa: http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-P-0009-V1_0_0_CRWG_Defs.pdf

[14] Rawat, A.S., Anand P., Chen H. & Varshney, P.K. *Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks*. IEEE Transactions on Signal Processing, 2011. Vol 59 (2), p. 774-786. ISSN 1941-0476.

[15] Siironen, S. *Palvelunestohyökkäyksen vaikutukset ohjelmisto-ohjatun tietoverkon ohjaimiin*. Pro gradu -tutkielma. Jyväskylä, 2018. Jyväskylän yliopisto, Informaatioteknologian tiedekunta. 91 s.

[16] Tuukkanen, T. *Ohjelmisto-ohjatut tietoverkot liikkeen mahdollistajana kyberpuolustuksessa*. Kirjassa: Heiskanen, M. & Valkola, E. (toim.). Kyberajan Viestitaktiikka. Kerava: Viestiupseeriyhdistys ry ja Maanpuolustuksen Viestisäätiö, 2018. 232 s. ISBN 978-952-94-0963-1.

[17] Thomas, R.W., Friend, D.H., DaSilva, L.A. & MacKenzie, A.B. *Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives*. IEEE Communication Magazine, 2006. Vol. 44 (12), p. 51-57. ISSN 1558-1896.

[18] Valvanne, J. *Ad-Hoc-verkot: Projektit, protokollat ja reititys*. Opinnäytetyö. Helsinki, 2014. Metropolia Ammattikorkeakoulu, Tietotekniikka, Tietoverkot. 36 s.

[19] Bouet, M., Phemius, K. and Leguay, J. *Distributed SDN for Mission-Critical Networks*. In: MILCOM 2014, IEEE Military Communications Conference. Baltimore, Maryland, USA, 6-8 October 2014. p. 942-948.

[20] Spencer, J., Worthington, O., Hancock, R. and Hepworth, E. *Towards a Tactical Software Defined Network*. In: 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23.-24. May 2016. p. 1-7. ISBN 978-1-5090-1777-5.

[21] Kärkkäinen, A. *A cyber security architecture for military networks using a cognitive network approach*, Diplomityö, Helsinki, 2013. Maanpuolustuskorkeakoulu, Yleisesiupseerikurssi. 114 p.

[22] Watson, S. & Willink, T. *Vulnerabilities in military dynamic spectrum access radio networks*. Ottawa: Defence Research and Development Canada – Ottawa Research Centre, 2018. 31 p.

[23] ITU-T X.1038. *Security requirements and reference architecture for software-defined networking*. Recommendation. Series X: Data Networks, Open System Communications and Security, Telecommunication Standardization Sector of ITU, 2016. 24 p.

[24] 1915.1. Standard for Software Defined Networking and Network Function Virtualization Security. 2017. IEEE-projekti 1915.1. IEEE Standards Association.

[25] Qiao Y, Yu F. R., Gong, Q. & Li J. *Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges*. IEEE Communications Surveys & Tutorials, 2016. Vol. 18 (1), p. 602–622. ISSN: 1553-877X.

[26] ONF TR-511. *Principles and Practices for Securing Software-Defined Networks*. Technical Recommendations. Open Networking Foundation. 2015. 27 p. Saatavissa: https://www.opennetworking.org/software-defined-standards/archives/

[27] ONF TR-529. *Security Foundation Requirements for SDN Controllers*. Technical Recommendations. Open Networking Foundation. 2016. 18 p. Available: https://www.opennetworking.org/software-defined-standards/archives/

[28] ONF TR-530. *Threat Analysis for the SDN Architecture*. Technical Recommendations. Open Networking Foundation. 2016. 21 p. Available: https://www.opennetworking.org/software-defined-standards/archives/

[29] Namal, S., Ahmad, I., Gurtov, A. & Ylianttila, M. *Enabling Secure Mobility with OpenFlow*. In: 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 11-13. Nov 2013. p. 1-5. ISBN 978-1-4799-2781-4

[30] Lo, B.F. *A Survey of Common Control Channel Design in Cognitive Radio Networks*. Amsterdam: Elsevier Physical Communication, 2011. Vol 4 (1), p. 26-39. ISSN 1874-4907.

[31] Masri, A.M., Chiasserini, C.-F., Casetti, C. & Perotti, A. *Common Control Channel Allocation in Cognitive Radio Networks through UWB Communication*. Journal of Communications and Networks, 2012. Vol. 14 (6), p. 710-718. ISSN 1976-5541.

[32] Koslowski, S., Elsner, J.P., Couturier, S., Keip, C. & Bettinger, O. *Distributed Localized Interference Avoidance for Dynamic Frequency Hopping ad hoc Networks*. In: 2013 Wireless Innovation Forum Conference on Communications Technologies and Software Defined Radio, Washington D.C., USA, 8-10. Jan 2013. Available: https://www.cel.kit.edu/download/SDR-WInnComm-2013_KoslowskiEtAl.pdf

[33] Mirhoseninejad, S., Berangi, R & Fathy, M. *Improving saturation capacity through verification of common control channel mechanism in cognitive radio ad-hoc networks*. In: Proceedings of the 4th International Conference on Computer and Knowledge Engineering, ICCKE, Dec 2014. p. 515-518.

[34] Rauschen, D., Couturier, S., Adrat, M., Antweiler, M., Elders-Boll, H. *Cooperative Spectrum Sensing for a Real-Time Cognitive Radio Demonstrator*. In: Symposium on Cognitive Radio and Future Networks, Hague, Netherlands, 12-13. May 2014. NATO STO-MP-IST 123 RSY-029.

[35] Mukherjee, T. & Nath, A. *Cognitive Radio Network Architecture and Security Issues: A Comprehensive Study*. International Journal of Advanced Research in Computer Science and Software Engineering, 2015. Vol. 5 (6), p. 124-133. ISSN 2277 128X.

[36] Kalaiselvan, C. & Kavitha, K. *An Advanced Security Enhancements for Cognitive Radio Networks with Trust Management*. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2015. Vol. 4 (5), p. 4816-4822. ISSN 2278 –8875.

[37] Carlin, B. P. & Louis,T. A. *Bayes and Empirical Bayes Methods for Data Analysis*. 2nd ed. London: Chapman & Hall, 1996. 440 p. ISBN 978-1584881704.

[38] Shafer, G. *A Mathematical Theory of Evidence*. USA, Princeton: Princeton University Press, 1976. 314 p. ISBN 0-608-02508-9.

[39] Niskanen, V. A. *Sumea logiikka: Kirkasta älyä ja mallinnusta*. Helsinki: WSOY, 2003. 258 s. ISBN 951-0-28731-8.

[40] Marti, S., Giuli, T.J., Lai, K. & Baker, M. *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*. In: Pickholtz, R., Das, S.K., Cáceres, R., Garcia-Luna-Aceves, J.J. (chairmen): MobiCom00: The 6th Annual International Conference on Mobile Computing and Networking. New York: Association for Computing Machinery, 2000. p. 255-265. ISBN 978-1-58113-197-0.

[41] Smarandache, F. & Dezert, J. *Advances and Applications of DSmT for Information Fusion*. Ann Arbor: American Research Press Rehoboth, 2004, 2006, 2009. Vol. 1-3. 411 p. ISBN: 1-931233-82-9.

[42] Pasivirta, P, Kosola, J. *Vaatimusten hallinnan soveltaminen Puolustusvoimissa*. Helsinki: Pääesikunta, Sotatalousosasto, 2004. 159 s. ISBN 951-25-1548-2.

[43] Vilpas, P. *Kvantitatiivinen tutkimus*. Opetusmateriaali. Helsinki: Metropolia-ammattikorkeakoulu. Saatavissa: https://users.metropolia.fi/~pervil/kvantsu/Moniste.pdf

[44] Heikkilä, T. *Tilastollinen tutkimus*. 5. painos. Helsinki: Edita Prima, 2004. 327 s. ISBN 951-37-4135-4.

[45] Koivisto, J. & Tuukkanen, T. *Comprehensive Capability Meta Model Tested by a Cognitive Radio*. In: MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23-25. Oct. 2017. p. 731-737. ISBN: 978-1-5386-0595-0.

[46] Jyväskylän yliopisto. *Tilastollisesti kuvaava analyysi*. [viitattu 20.3.2020]. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/tilastollisesti-kuvaava-analyysi

[47] Mellin, I. *Tilastolliset menetelmät*. Helsinki: Aalto-yliopisto, 2006. 50 s. [viitattu 21.3.2020] Saatavissa: https://math.aalto.fi/opetus/sovtoda/oppikirja/Johdanto.pdf

[48] Pantsar, L. *Upseerikoulutuksen tieteellisyydestä*. Kirjassa: Lappalainen, E. & Jormakka, J. (toim.). Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa. Helsinki: Maanpuolustuskorkeakoulu, Tekniikan laitos, 2004. s. 7−15. ISBN 951-25-1540-7.

[49] Hiltunen, L. *Validiteetti ja reliabiliteetti*. Opetusmateriaali. Jyväskylä: Jyväskylän yliopisto. [viitattu 22.3.2020]. Saatavissa: http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf

[50] DOTMLPFIi tarkistuslista - osatekijöiden kuvaukset, Teoksessa: Suorituskyvyn käsitemalli, PVOHJEK-PE – PESUUNNOS HJ108. Helsinki: Pääesikunnan suunnittelu-osasto, 21.11.2013. Liite 2.

LIITTEET

LIITE 1. Työssä käytetyt yleisimmät käsitteet, määritelmät ja lyhenteet

Kognitiivinen radio (CR - *cognitive radio*): älykäs langaton viestintäjärjestelmä, joka on tietoinen ympäröivästä ympäristöstään ja kykenee mukauttamaan asetuksiaan automaattisesti sähkömagneettisessa spektrissä tapahtuvien muutosten pohjalta. Ärsykkeet aiheuttavat vastaavia muutoksia tiettyihin toimintaparametreihin (esim. lähetysteho, kantoaaltotaajuus ja modulaatio) reaaliajassa, ottaen huomioon kaksi päätavoitetta: erittäin luotettavat yhteydet (ajallisesti ja alueellisesti) sekä radiospektrin tehokkaan hyödyntämisen. [1, kpl 2, s. 2]

Kognitiivinen tietoliikennejärjestelmä: Kognitiivisella tietoliikennejärjestelmällä on kolme perusominaisuutta: tilannetietoisuus, oppimis- ja päätöksentekokyky sekä täysin kontrolloitavat tietoliikenneparametrit ja -asetukset, joista voidaan johtaa kognitiiviset perustoiminnot: havainnointi, oppiminen, päätöksenteko, itseohjautuvuus ja automaattinen konfiguroituminen. [3]

Kognitiivinen radioverkko (CRN, *Cognitive Radio Network*): kognitiivisista solmuista koostuva langaton tietoliikenneverkko, joka voi tunnistaa ympäristönsä, säätää verkon käyttäytymistä vastaavasti ja oppia aiemmista kokemuksista. [1]

Ensisijainen käyttäjä (PU - *primary user*): taajuuksien käyttäjä, jolla on korkeammat prioriteettioikeudet dynaamisessa spektrinkäytössä spektrin tietyn osan käytössä. Ensisijaisilla käyttäjillä on käyttöoikeus verkkoon. [1, kpl 2, s. 5; YE, s. 3]

Toissijainen käyttäjä (SU - *secondary user*): verkon käyttäjä, jolla on alhaisempi prioriteetti, ja joka siksi hyödyntää dynaamista spektrinkäyttöä niin, että se ei aiheuta häiriöitä ensisijaisille käyttäjille. Toissijaisilla käyttäjillä ei ole käyttöoikeutta verkkoon. [1, kpl 2; YE, s. 3] Siviili- ja kaupallisilla aloilla PU viittaa vakiintuneeseen käyttäjään *(incumbent)*. PU- ja SU-käsitteitä on ehdotettu käytettävän sotilaallisessa kognitiivijärjestelmässä sellaisena kuin se on määritelty siviili- ja kauppapuolella. Määritelmä voi liittyä verkon priorisointiin suhteessa toiseen, mutta myös palveluihin ja toimintoihin yhden verkon sisällä. [1, kpl 2, s. 5]

DSA (*dynamic system access):* dynaaminen spektrinkäyttö DSA mahdollistaa toisiokäyttäjien ensisijaiselle käyttäjälle allokoidun taajuusresurssin jakamisen. DSA:n myötä toisiokäyttäjien on mahdollista jakaa taajuusresurssia aiheuttamatta häiriötä samalla taajuusalueella jo oleville järjestelmille. DSA:ssa radio suorittaa jatkuvaa spektrin analysointia, jonka jälkeen se erottelee signaalit kohinasta päättelemällä vastaanottamiensa spektrin näytteiden perusteella, ovatko signaalit päällä vai pois päältä. [9, s. 22-29]

SS ja DSS (*spectrum sensing & distributed spectrum sensing)*: taajuushavainnointi (SS) on avainroolissa kognitiivisen radion toiminnan kannalta. Yksittäisten taajuushavaintojen vaikutuksien vähentämiseksi on ehdotettu taajuuksien tunnistamisen jakelu- ja yhteistyömallia, eli hajautettua taajuushavainnointia (DSS). Hajautetussa taajuushavainnoinnissa joukko kognitiivisia radioita muodostavat verkon, jossa lopullinen päätös taajuuden käytettävyydestä tehdään kaikkien kognitiivisten radioiden vastaanottaman tiedon perusteella. [14, s. 1]

Kontrollikanava (CCC, common control channel): Kognitiivinen radioverkko vaatii tueksi yhteisen kontrollikanavan, joka toimii avainelementtinä koko verkon yhteisen ohjaamisen suhteen. Kognitiivisten radioverkkojen kokonaisuudet, kuten esim. verkonmuodostuminen, taajuushavainnointitulokset sekä tarvittavat kanavamuutokset vaativat kontrolliliikennettä. Kontrollikanava mahdollistaa verkonlaajuiset parametrien uudelleenmääritykset. [1, kpl 4]

SDN (*software defined network*): Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri (SDN) tarkoittaa tietoverkon hallitsemista ja ohjaamista ohjelmistolla. Arkkitehtuuri on jaettu kolmeen tasoon, joista alimpana on verkkoelementtitaso (*data plane*), jonka lisäksi on sekä hallintataso (*control plane*) että verkkosovellustaso (*application plane*). Arkkitehtuuri tukee kolmea pääperiaatetta: ohjauslogiikan ja tiedonsiirron erottaminen, loogisesti (ei välttämättä fyysisesti) keskitetty ohjaus ja verkkotoimintojen ohjelmoitavuus. [1, kpl 4 s. 41-47; 2, s. 27; 15, s. 1-5; 16, kpl 4.4]

OpenFlow: OpenFlow-protokolla on yleisin ja standardoitu protokolla, jota käytetään ohjaimen ja kytkinten välillä. Kun tietovuo saapuu kytkimeen, kytkin välittää ensimmäisen paketin (paketit) ohjaimeen. Ohjain tekee päätökset pakettien reitittämisestä ja asentaa nämä päätökset kytkimeen käyttämällä OpenFlow-protokollaa. Päätökset ovat vuosääntöjen muodossa, jotka kuvaavat sen tietovuon sisältävien pakettien toiminnot. Vuosäännöt tallennetaan kytkimien vuotaulukoihin ja ohjain voi muuttaa vuosääntöjä milloin tahansa. [2, s. 28]

API (*application programming interface*): Ohjelmointirajapinta, jonka päätarkoituksena on tarjota käyttömahdollisuus yleisimmille toiminnoille.

LIITE 2. Kyselyyn vastanneet asiantuntijat

Asiantuntija	**Organisaatio**	**Kategoria**
Petteri Hemminki	PVTUTKL	Puolustusvoimat
Topi Tuukkanen	PVTUTKL (evp)	Puolustusvoimat
Anders Furu	PVTUTKL	Puolustusvoimat
Erno Pasanen	PVTUTKL	Puolustusvoimat
Heikki Rantanen	PVTUTKL	Puolustusvoimat
Kimmo Heinäaro	PV PE	Puolustusvoimat
Timo Bräysy	Oulun yliopisto	Tiedeyhteisö
Pekka Susi	Cojot Oy	Teknologiateollisuus

Liite 3. Kyselyn ensimmäisen kierroksen kyselylomake

Pro gradu -tutkimuksen ”Kognitiivisen (taktisen) tietoliikennejärjestelmän kyberturvallisuuden vaatimukset ja toteutusvaihtoehdot” kyselyn ensimmäinen kierros (avoimet kysymykset):

Kognitiivinen radio, ja -radioverkko

1. Millaiset ominaisuudet mielestäsi tekevät tietoliikenneverkosta kognitiivisen?
2. Kognitiivinen radioverkko koostuu solmuista, joista löytyy kognitiivinen radio. Mitä ominaisuuksia/toiminnallisuuksia tämä radio voisi sisältää?
3. Mitä kognitiivisia ominaisuuksia taktiseen radioverkkoon voisi kuulua?
4. Mitä hyötyjä tai uhkia kognitiivisuus tietoliikennejärjestelmissä voisi muodostaa sotilaallisessa kontekstissa?

Kognitiiviseen tietoliikenneverkkoon kohdistuvat kyberuhkat

5. Millaisia kyberuhkia voisi kohdistua kognitiiviseen tietoliikenneverkkoon?
6. Suurvallat käyttävät termiä Cyber-EW, jolla tarkoitetaan elektronisen sodankäynnin integroitumista kyberulottuvuuden kanssa. Millaisia uhkia tämänkaltaiset hyökkäysvektorit voisivat aiheuttaa kognitiiviselle radioverkolle?

Kognitiivisen tietoliikenneverkon kyberturvallisuuden kehittäminen

7. Mitä vaatimuksia kyberturvallisuuden suhteen tulisi asettaa nimenomaan kognitiiviselle tietoliikenneverkolle?
8. Millaisia toteutusvaihtoehtoja kognitiivisen tietoliikenneverkon kyberturvallisuuden parantamiselle voisi löytää?

VAPAA SANA JA MAHDOLLISET KOMMENTIT:

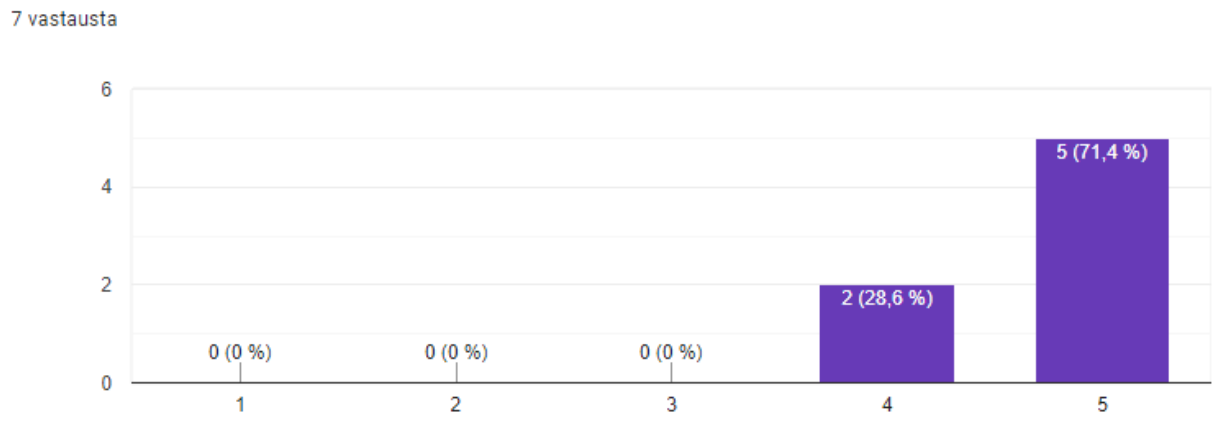
Liite 4. Kyselyn toisen kierroksen väittämät ja vastausjakaumat

1. Kognitiivinen radio ja kognitiivinen tietoliikenneverkko

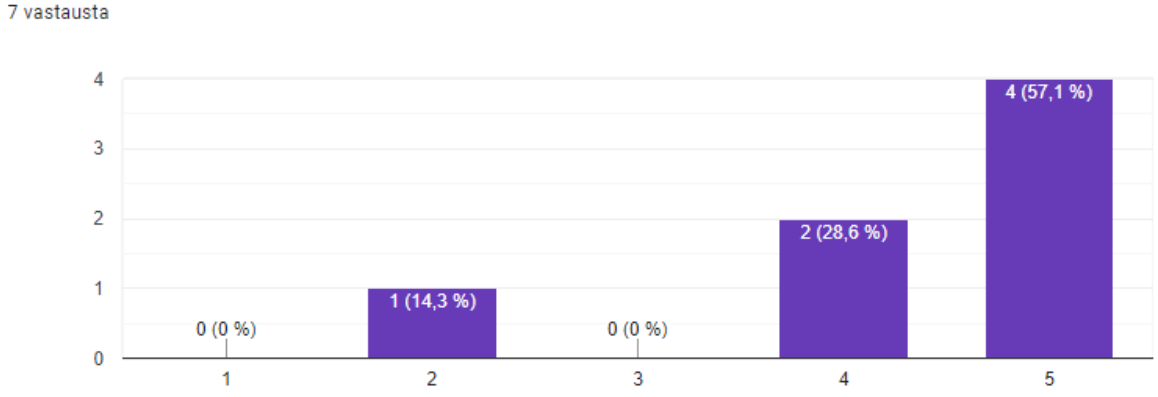
Vastausvaihtoehdot:

	1	2	3	4	5	
Täysin eri mieltä	○	○	○	○	○	Täysin samaa mieltä

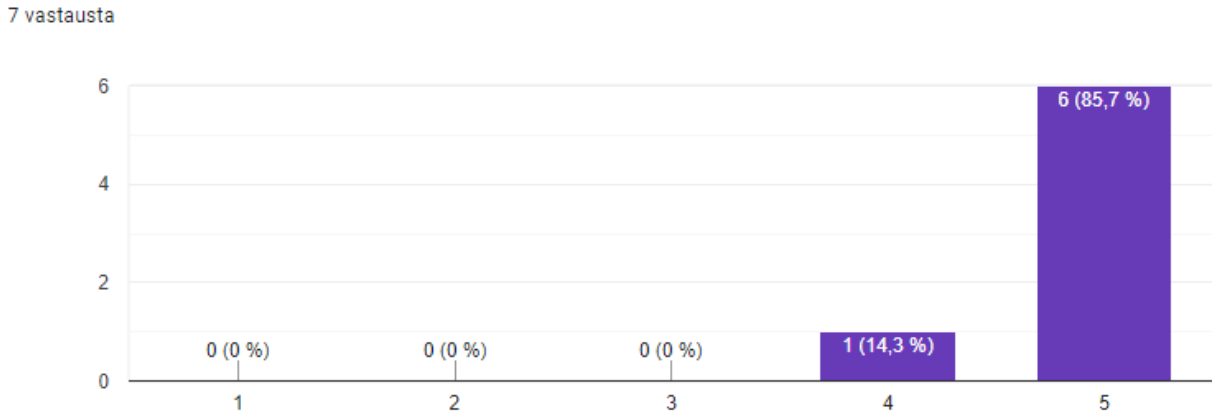
1. Kognitiivisesta radiosta tulee löytyä vähintään seuraavat ominaisuudet: 1. Dynaaminen spektrinkäyttö, DSA, joka mahdollistaa toisiokäyttäjien (secondary users) ensisijaiselle käyttäjälle (primary user) allokoidun taajuusresurssin jakamisen. 2. Yhteyksien adaptiivisuus ja radioresurssien hallinta (RRM), jolla tarkoitetaan prosessia, jossa radion eri parametreja, kuten teho, taajuus ja hypytysnopeus, hallitaan järjestelmätasolla ohjelmistollisesti. 3. Itsenäisesti organisoituva verkko (SON), jolla tarkoitetaan verkkoa, joka voi automaattisesti laajentua, muuntua ja konfiguroitua sekä optimoida verkon peittoaluetta, kapasiteettia, topologiaa, taajuusallokointia ja kaistanleveyksiä. Optimointikyky perustuu verkon kykyyn reagoida häiriöihin (kuten ELSO), signaalin vahvuuteen, paikkaan, viestiliikenteen toimintamalliin sekä muihin ympäristöllisiin ominaisuuksiin.



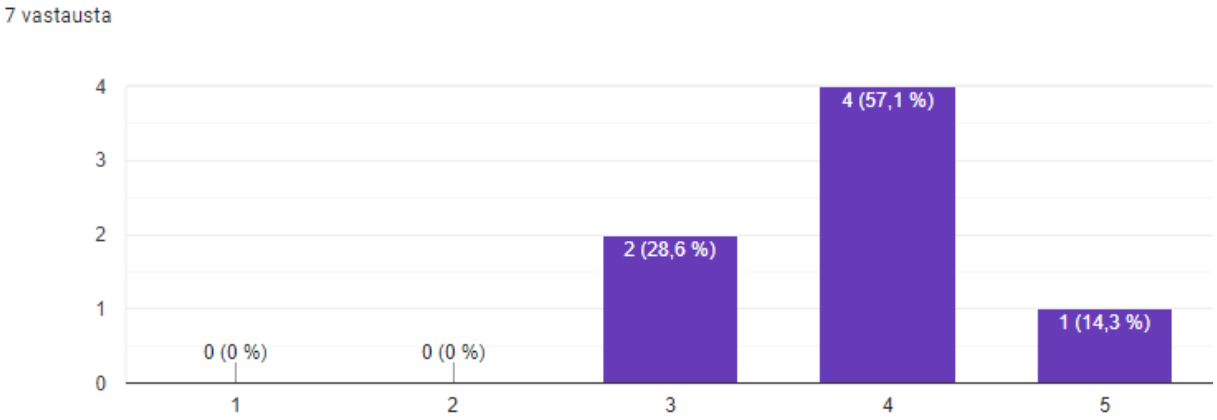
2. Kognitiivisella radiolla tulee olemaan merkittävä rooli elektronisessa sodankäynnissä.



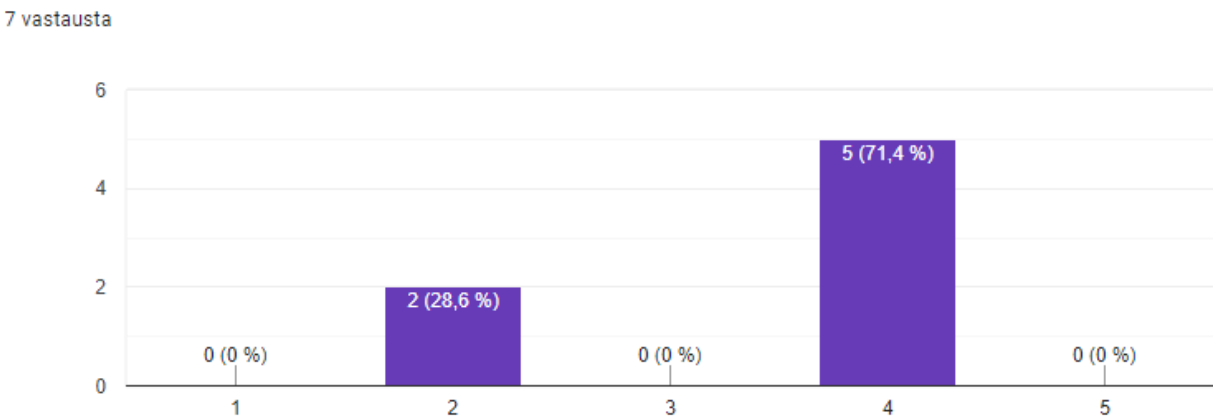
3. Jotta radioverkko voi mukautua muuttuvaan ympäristöön, tulee kognitio tuoda mukaan koko verkkoon, ei vain päätelaitteeseen.



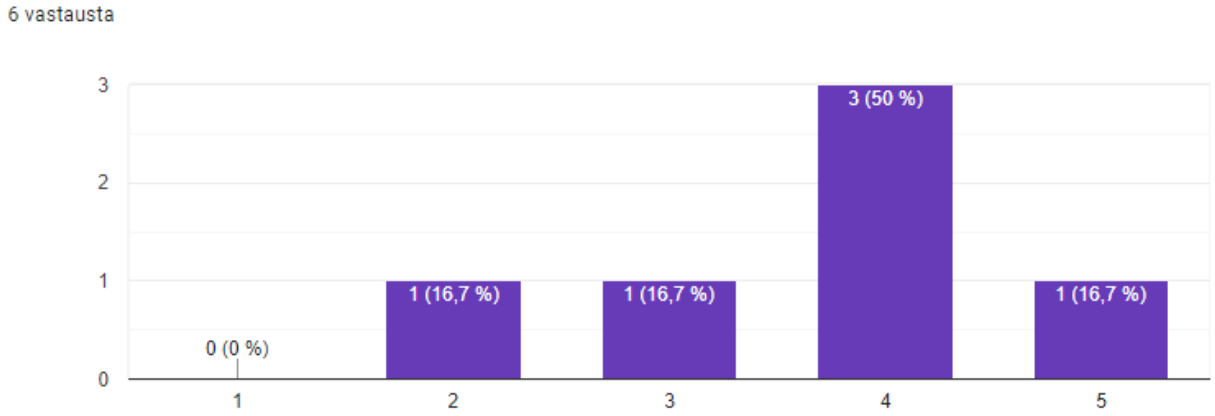
4. Nykyiset verkkolaitteet vaikeuttavat verkonlaajuisten käytäntöjen konfigurointia ja uusien, mukautuvien ominaisuuksien kehittämistä. Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri (SDN, Software Defined Networking) on yksi ratkaisumalli edellä kuvattuihin ongelmiin.



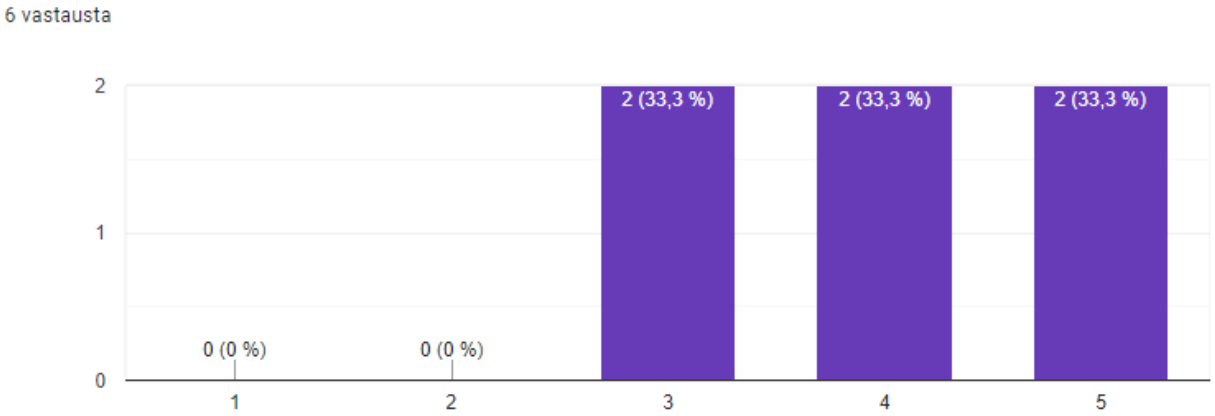
5. SDN-arkkitehtuurin olennainen osa on keskitetty ohjainohjelmisto, jolla voidaan hallita koko tietoverkkoa. Arkkitehtuurissa verkkolaitteista on poistettu kaikki logiikka, jolloin ne sisältävät vain liikenteenvälitykseen vaadittavat toiminnot. Verkon älykkyys on keskitetty ylemmille hallinta- (control plane) ja verkkosovellustasoille (application plane).



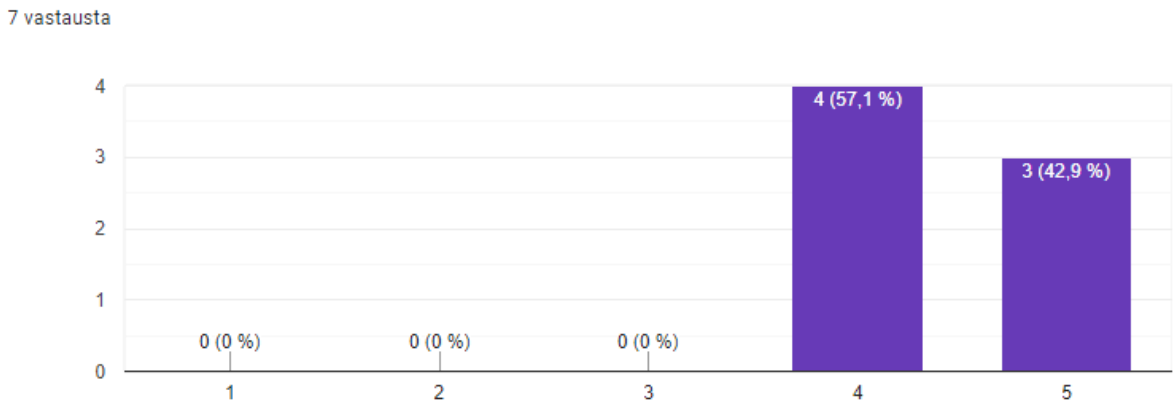
6. Ohjelmisto-ohjattu verkko perustuu kolmeen perusperiaatteeseen: I) fyysisen ja ohjelmistokerroksen erottamiseen, II) loogisesti keskitettyyn ohjaukseen ja III) verkkotoimintojen ohjelmoitavuuteen.



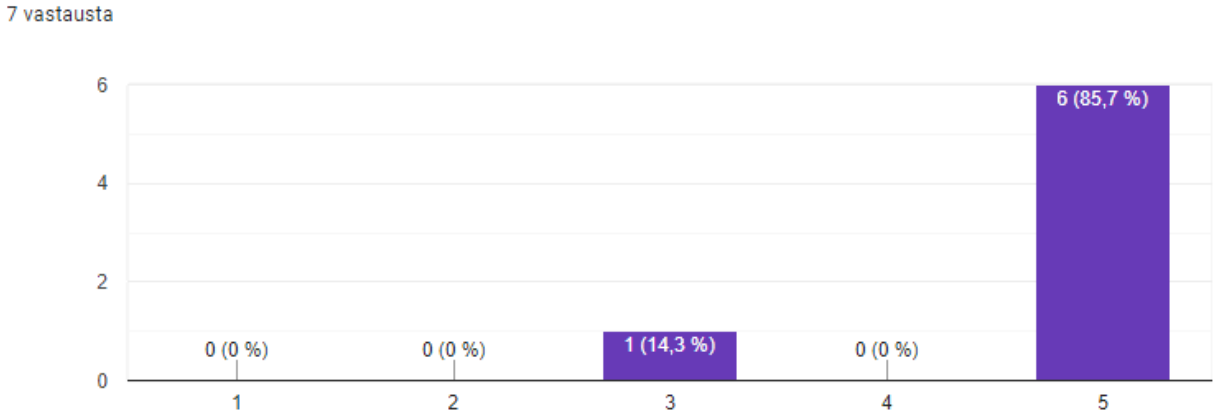
7. Ohjelmisto-ohjauksen arkkitehtuuri muodostuu kahdesta pääkomponentista: hallintatasolla olevasta ohjaimesta (SDN Controller, SDN-C), jota voidaan kutsua myös verkkokäyttöjärjestelmäksi (NOS, network operating system), ja liikennetasolla olevasta liikennettä välittävästä laitteesta (SDN Forwarding Element, SDN-FE).



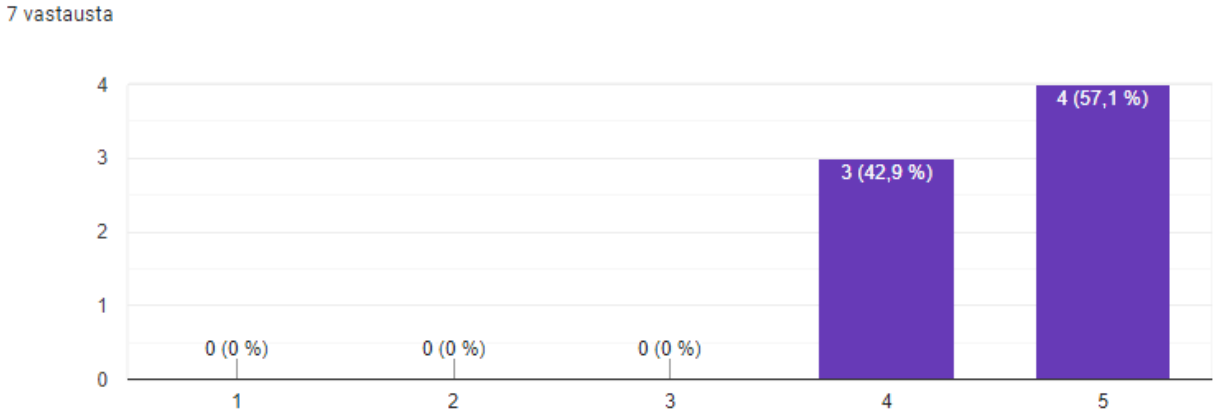
8. Kognitiivinen tietoliikennejärjestelmä eroaa ohjelmisto-ohjatusta tietoliikenneverkosta, koska vaikka SDN voi säätää nopeasti verkon käyttäytymistä, siitä puuttuu kognitio ja tietoisuus ympäristöstä ja siten myöskin tieto siitä, mihin sopeutua.



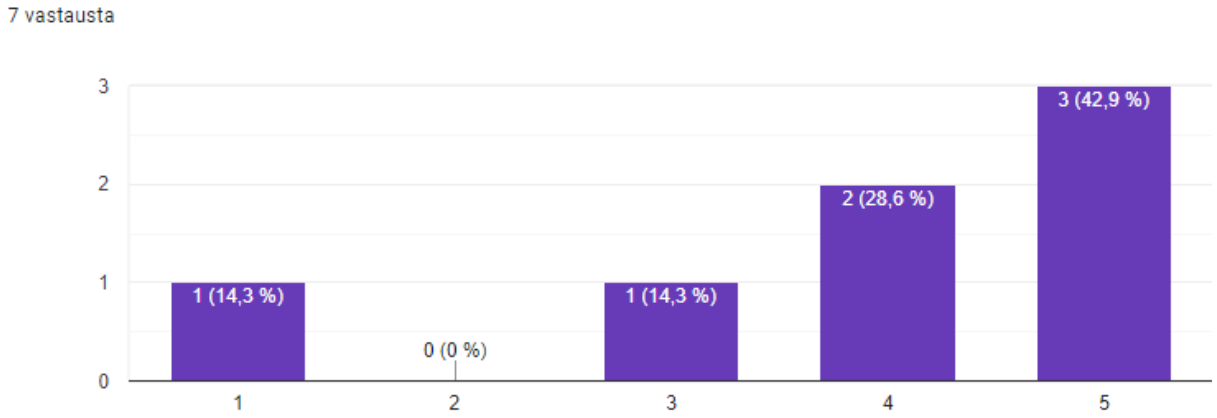
9. Kognitiivinen tietoliikennejärjestelmä eroaa myös kognitiivisesta radiosta (CR), koska kognitiivinen radio on tietoinen vain paikallisesta spektriympäristöstä ja siten tarkoitettu optimoimaan vain point-to-point -yhteydet, eikä se voi optimoida kokonaisuutta koko verkon suorituskyvyn suhteen.



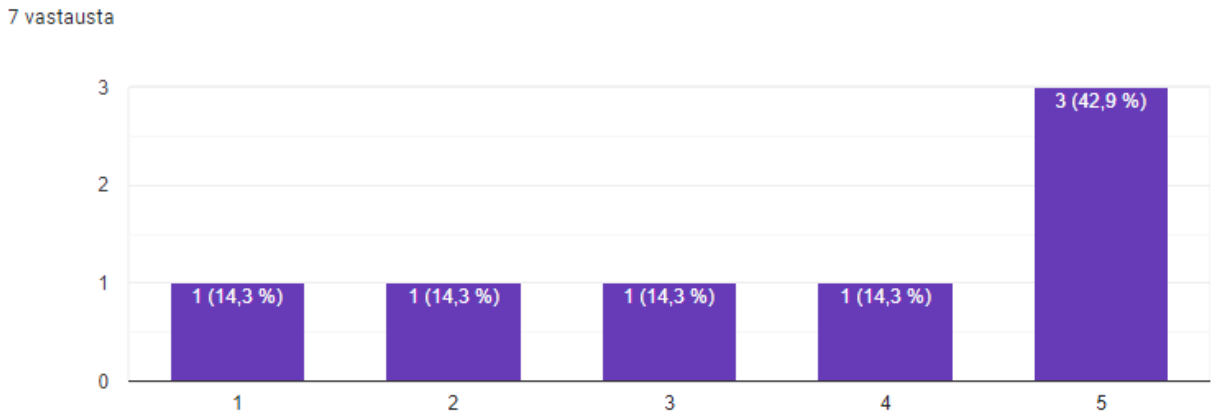
10. Kognitiivisella verkolla on kolme perusominaisuutta: tilannetietoisuus, oppimis- ja päätöksentekokyky sekä täysin kontrolloitavat tietoliikenneparametrit ja -asetukset, joista voidaan johtaa kognitiiviset perustoiminnot: havainnointi, oppiminen, päätöksenteko, itseohjautuvuus ja automaattinen konfiguroituminen.



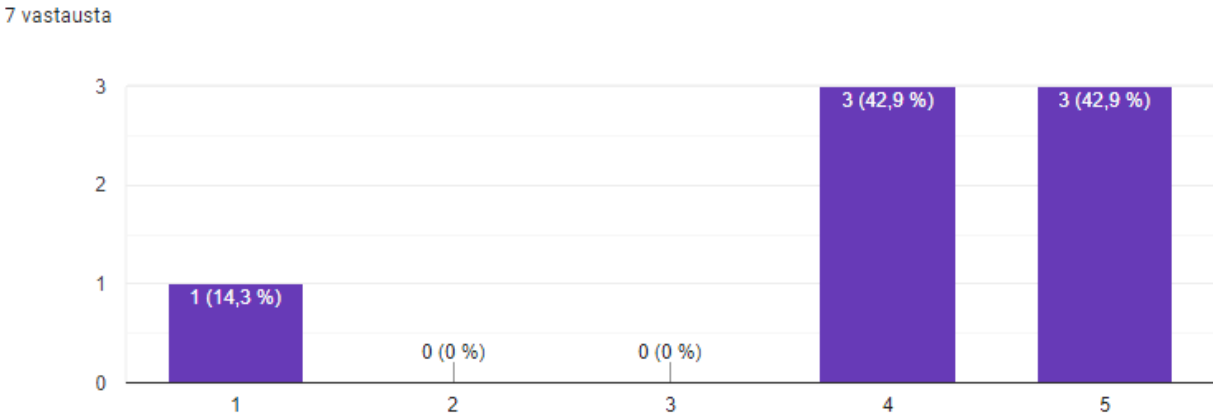
11. Kognitiivisen tietoliikenneverkon määritelmään kuuluu tavoitteellisuus, ns. ”päästä päähän” -malli (end-to-end). Tämä päästä-päähän -termi sisältää tässä yhteydessä kaikki ne verkon osat, jotka tarvitaan datavirran siirtämiseen. Päästä-päähän -ketju voi muodostua esimerkiksi aliverkoista, reitittimistä, kytkimistä, virtuaaliyhteyksistä, salausjärjestelmistä, siirtomedioista, rajapinnoista tai aaltomuodoista. Päästä-päähän -tavoite saa aikaan verkon laajuisen kognitiivisen luonteen, mikä edellyttää edellä mainittujen elementtien olevan ohjelmistopohjaisesti konfiguroitavissa. Ilman näitä tekijöitä järjestelmä voi sisältää kognitiivisia osia (esimerkiksi kognitiivinen radio), mutta järjestelmä ei ole kokonaisuudessaan kognitiivinen tietoliikenneverkko.



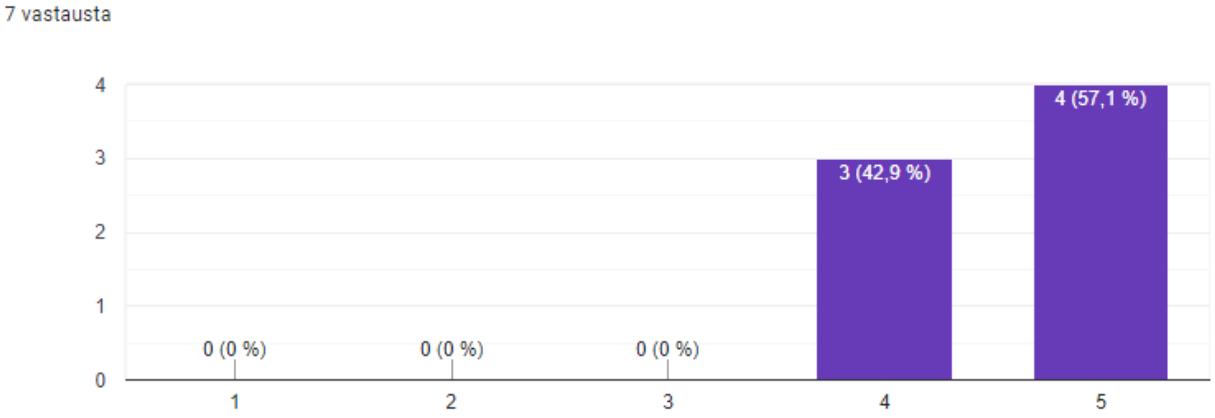
12. Kognitiivisessa radioverkossa jokaisessa solmussa kerätty tieto tulisi kyetä jakamaan verkonlaajuisesti ja päätökset tulee kyetä tekemään hajautetulla tavalla.



13. Kognitiivinen verkko vaatii tueksi yhteisen kontrollikanavan (CCC, common control channel), joka toimii avainelementtinä koko verkon yhteisen ohjaamisen suhteen. Yhteistä kontrollikanavaa voidaan käyttää myös suorittaakseen koko verkon laajuisia toimintatavan uudelleenmäärityksiä.



14. Kognitiivinen tietoliikennejärjestelmä tarkoittaa verkonhallinnan suhteen sitä, että voidaan keskittyä itse tehtävän suorittamiseen joutumatta toteuttamaan vaikeita verkkomääritystehtäviä operaation aikana. Tästä syystä myös tekninen konfigurointi ennen operaatioita vähenee.



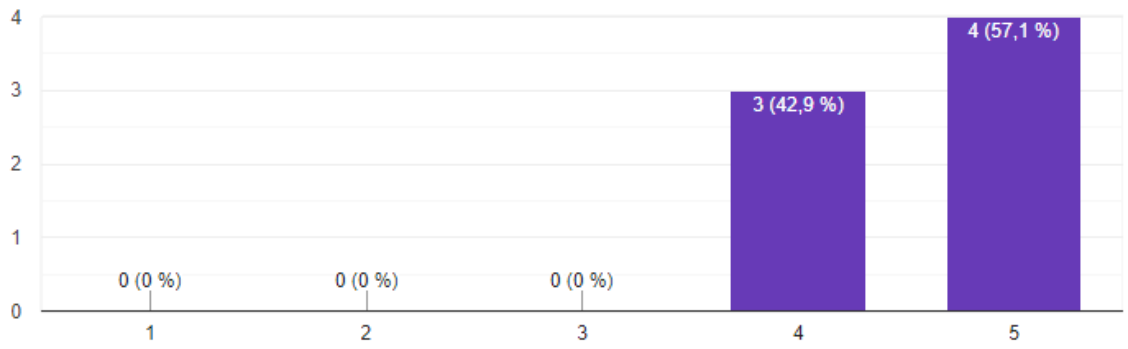
2. Kognitiiviseen taktiseen tietoliikenneverkkoon kohdistuvat uhkat

Vastausvaihtoehdot:

	1	2	3	4	5	
Ei merkittävää uhkaa	○	○	○	○	○	Erittäin merkittävä uhka

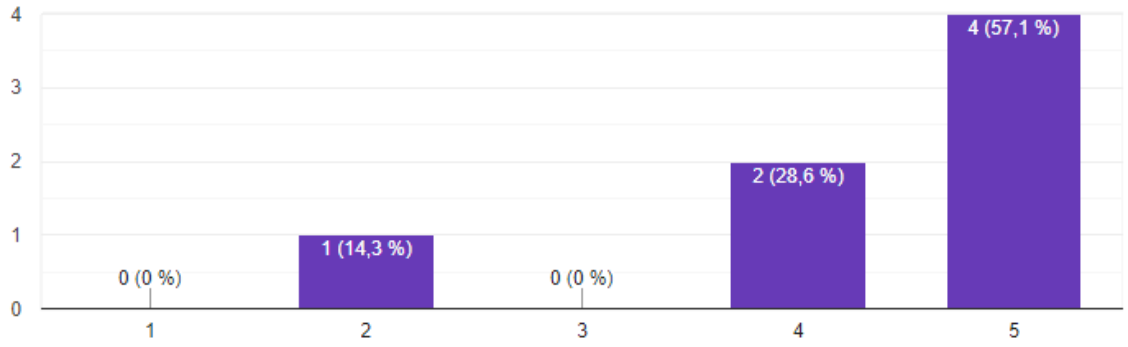
15. SDN:n ohjaimet voidaan jakaa edelleen keskitettyihin ja hajautettuihin ohjaimiin. Keskitetty ohjain hallitsee kaikkia verkon laitteita yhdestä paikasta käsin, ja sen toimintavarmuus on siten kriittinen. Keskitetty ohjaus voi muodostua kriittiseksi uhaksi (Single-Point-of Failure).

7 vastausta

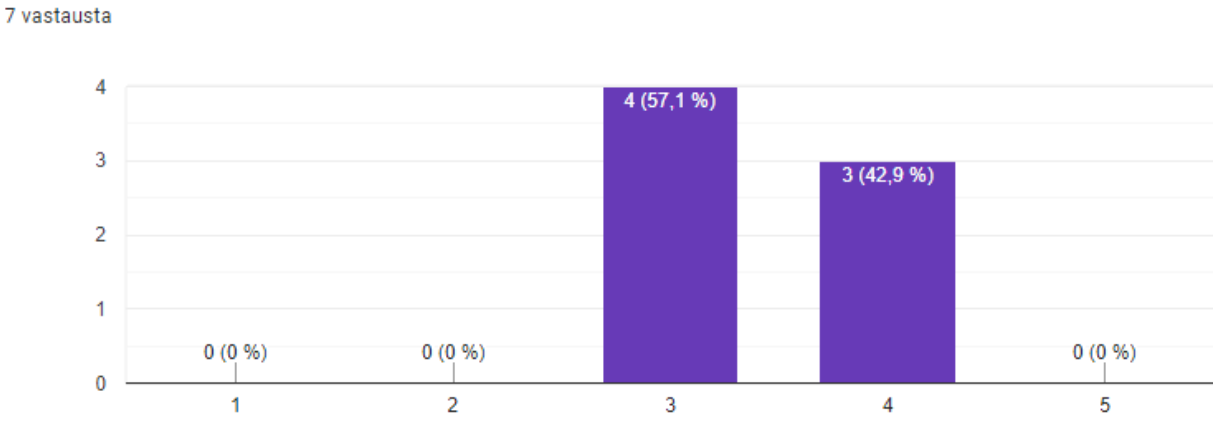


16. SDN-verkon uhkia ovat muun muassa keskitetyn hallinnan turvallisuuden takaaminen, ohjaimen ja verkkolaitteiden välisen viestinnän turvaaminen ja verkkosovellusten vahingollisen toiminnan estäminen.

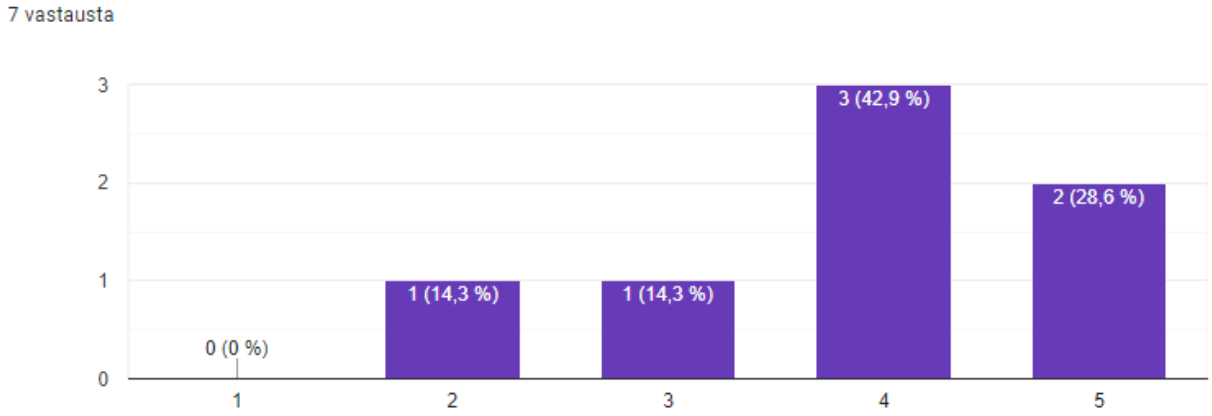
7 vastausta



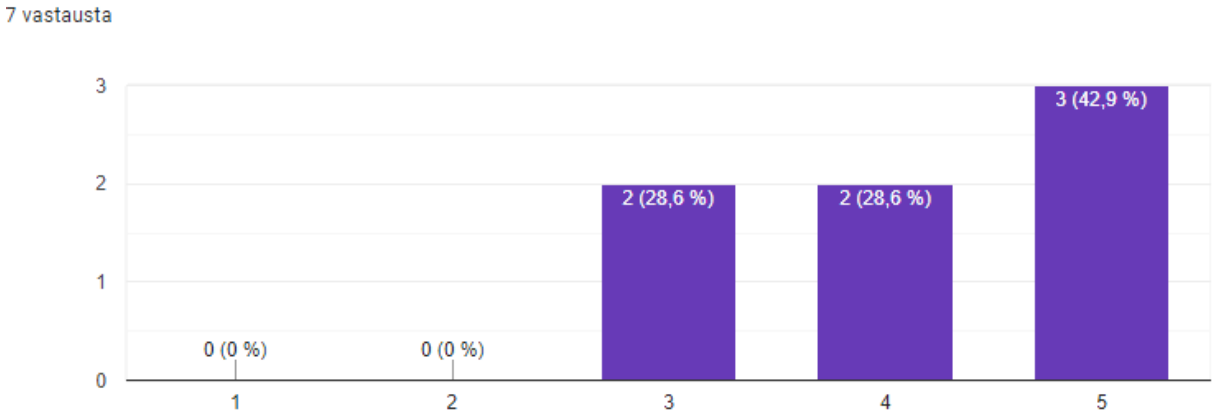
17. Kognitiivisen radioverkon hajautettu taajuushavainnointi DSS (Distributed Spectrum Sensing) muodostaa verkossa pullonkaulan vaihtaessaan spektrianturidataa, jolloin se vaatii luotettavat tietoliikenneyhteydet anturipäätelaitteiden ja päätöksiä suorittavan fuusiokeskuksen välillä.



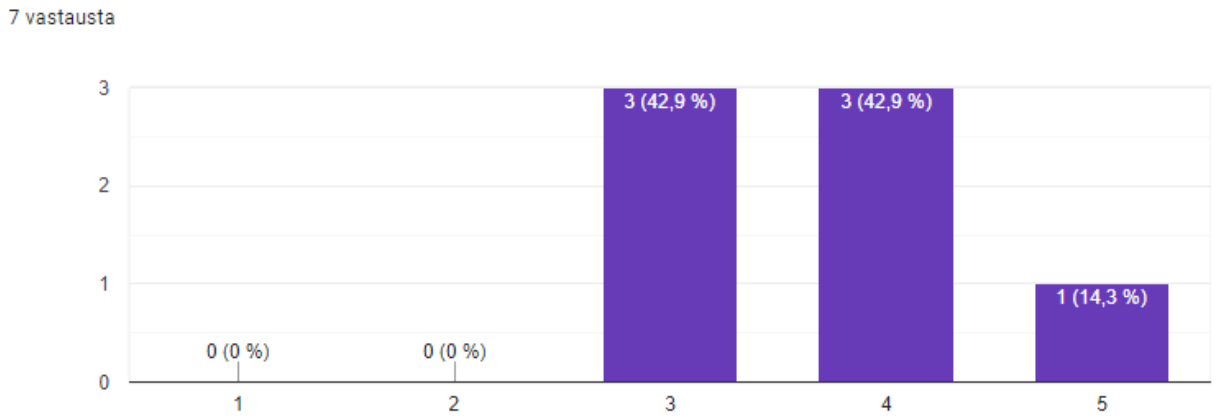
18. DSA-protokollia tai verkon taajuuspäätösprosessia voidaan manipuloida vastustajan etujen mukaisesti.



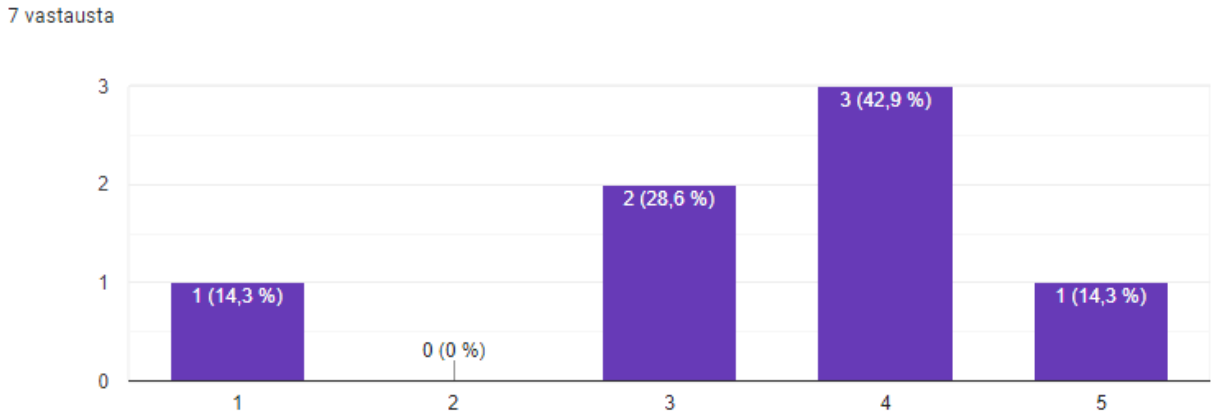
19. DSA muodostaa uudenlaisen uhkan ELSO:n näkökulmasta: mikäli radioverkkoa käytetään automaattisella kanavanvalinnalla, verkon havaitessa nykyisellä kanavalla kynnysarvoa suurempaa häiriötä, se vaihtaa toiseen käytettävissä olevaan kanavaan, jolla on vähemmän häiriöitä. Verkon kanavanvaihto on ennustettavissa, mikäli sen tiedetään olevan DSA-verkko, jolloin astustaja voi hyödyntää tätä ennustettavuutta. Toistuvat taajuusvaihdot heikentävät verkon suorituskykyä merkittävästi, koska yhteyden muodostumisesta uudelle kanavalle seuraa viivettä, jolloin hyötylähetettä ei voida lähettää, kun verkon resurssit kuluu kontrolliliikenteeseen. Kanavan vaihtamisnopeus on rajallinen, ja verkko kärsii häiriöistä, kunnes se toipuu uudella kanavalla. Verkon ja häirintäaseman suorituskyvystä riippuen, seurantahäirintä voi kokonaan estää palvelut verkossa. Vastustajan elektroninen häirintä voi myös havaita taajuuksien nykyisen käyttöasteen ja päättää sen perusteella, millä kanavalla verkkoa häiritään.



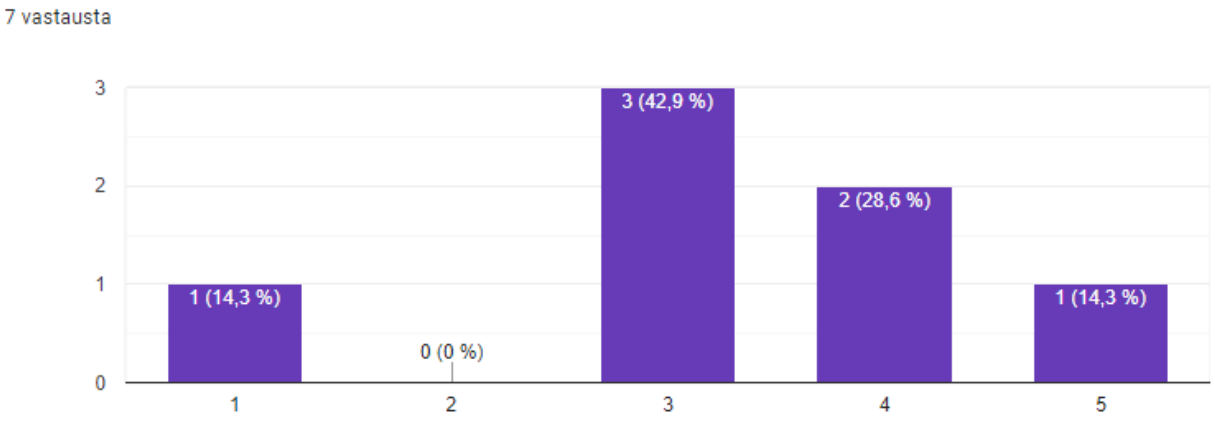
20. DSA luo myös seuraavanlaisen uhkan ELSO:n näkökulmasta: vastustaja voi saada käyttäjät valitsemaan tietty taajuuskanava (kanavat) ”laumakäyttäytymisellä”. Vastustaja saattaa tukkia kaikki mahdolliset taajuuskanavat paitsi yhden, jolloin tämä yksi kanava näyttää houkuttelevalta verkolle. Tämä taajuuskanava voi olla kanava, joka on vastustajalle helpoimmin havaittavissa. Vastustaja saattaa haluta myös pakottaa verkon tiettyyn spektrimääritykseen, joka mahdollistaa hyökkäyksen toisen vaiheen käynnistämisen. Tämä voi ilmetä häirintänä tietyillä verkon osan kanavilla liikenteen ohjaamiseksi kohti tietomurrettua/vihollisen hallussa olevaa solmua.



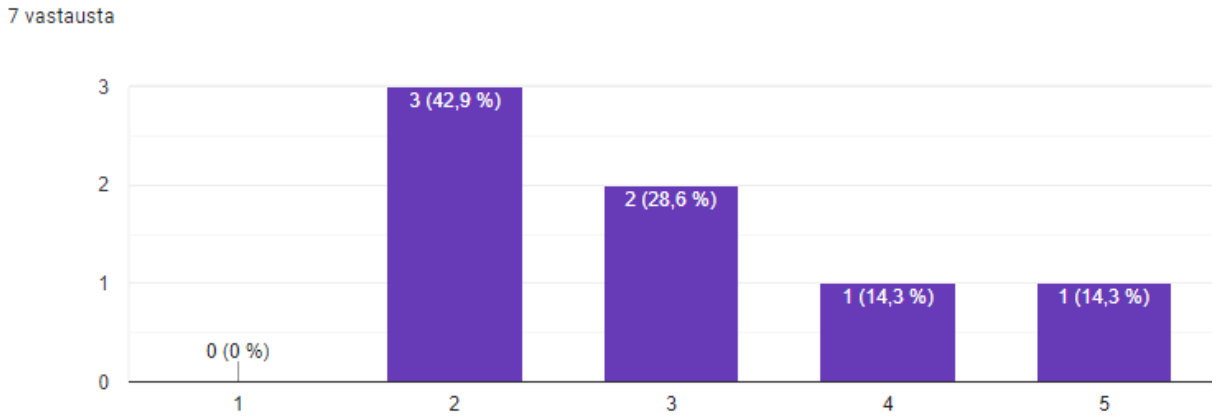
21. Ensisijaisen käyttäjän emulointihyökkäys muodostaa uhkan kognitiiviselle radioverkolle: Ellei verkko totea, että häirintälähete on läsnä, toisiokäyttäjien on oletettava, että häiriöt johtuvat ensisijaisesta käyttäjästä. Tämä johtaa toisiokäyttäjien spektrin vapauttamiseen, kunnes häiriötä ei enää ole. Tämä mahdollistaa vastustajan kanavien tukkimisen joko lähettämällä kohinaa, joka ylittää vain toisiokäyttäjien radioiden havaitsemiskynnyksen, tai lähettämällä ensisijaisen käyttäjän aaltomuotoa jäljittelevän signaalin aiheuttaen siten palvelunestohyökkäyksen. Tällaista hyökkäystapaa kutsutaan ensisijaisen käyttäjän emulointihyökkäykseksi.



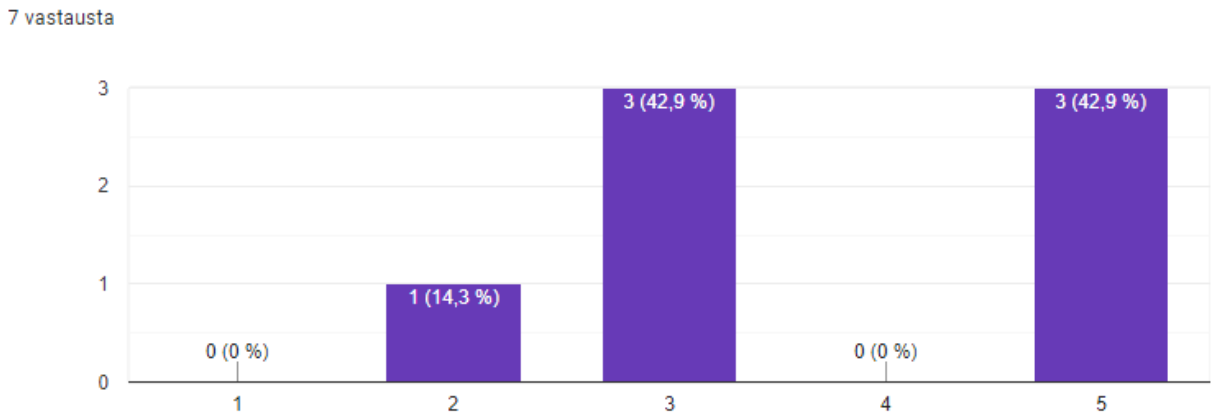
22. Hajautettua taajuushavainnointia (DSS) vastaan kohdistettu taajuushavainnoinnin väärentämishyökkäys (SSDF, spectrum sensing data falsification, kutsutaan myös Bysanttilaishyökkäykseksi, Byzantine attack) muodostaa uhkan verkon toiminnalle. Hyökkäyksessä hajautetulle taajuushavainnoinnille lähetetään vääriä taajuustunnistustietoja haitallisten toisiokäyttäjien toimesta häiritäkseen fuusiokeskuksen taajuushavainnointiprosessia. Virheelliset paikalliset taajuusmittaustulokset voivat aiheuttaa fuusiokeskuksen tekevän väärän päätöksen käytetyistä taajuuksista.



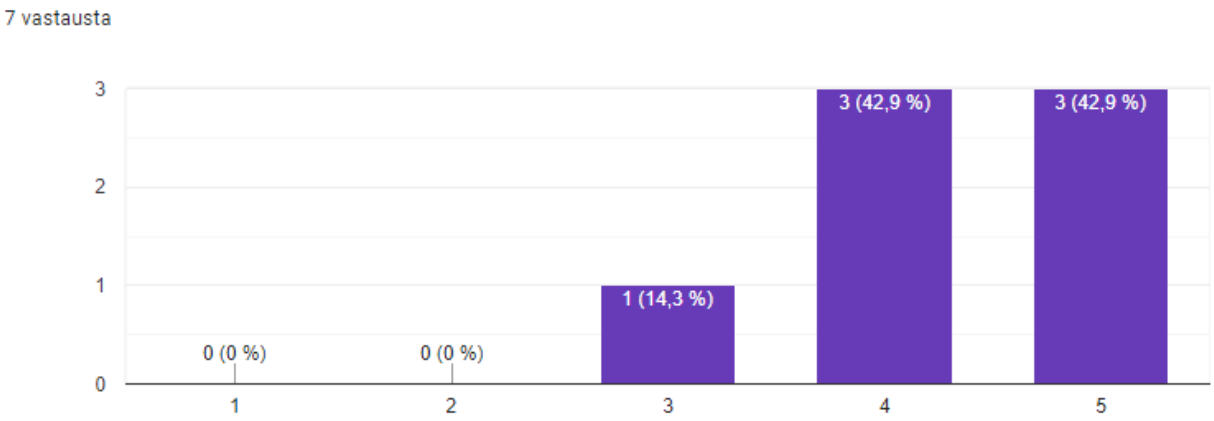
23. Kaikki ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tasot ja rajapinnat ovat alttiita palvelunestohyökkäyksille. Koska ohjaimen toiminta on erityisen kriittinen verkon toiminnan kannalta, muodostaa se houkuttelevan kohteen palvelunestohyökkäykselle. Palvelunestohyökkäys voidaan toteuttaa mm. lähettämällä ohjaimelle suuri määrä uusia tietovoita, tai lähettämällä suuri määrä paketteja tuntemattomille vastaanottajille.



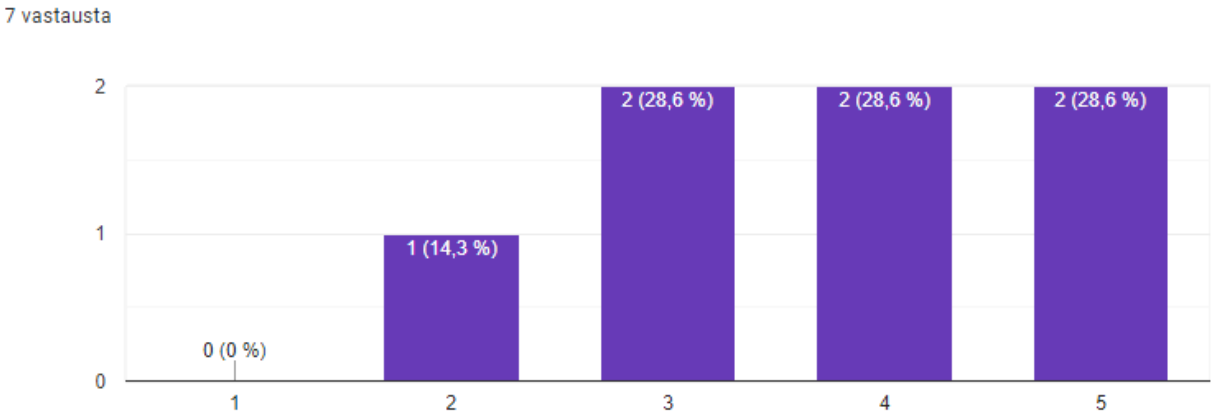
24. Kognitiivisiin radioverkkoihin liittyvät kokonaisuudet vaihtavat kontrolliliikennettä. Kontrolliliikennettä tarvitaan taajuuksien havainnointituloksien synkronoimiseksi ja yhteisten kanavien tunnistamiseksi. Myös kanavamuutoksista on neuvoteltava. Lisäksi kognitiiviset toiminteet eivät todennäköisesti rajoitu vain kanavan hallintaan. Kontrollikanavien suunnittelulle on löydettävissä neljä haastetta. Ensimmäinen haaste on välttää kontrollikanavan tukkeutuminen, toinen on häiriösietoisuus, kolmas on peittoalue ja neljäs on tietoturvallisuus. Ensimmäinen uhka, kontrollikanavan tukkeutuminen voi estää koko tietoliikennejärjestelmän toimimisen.



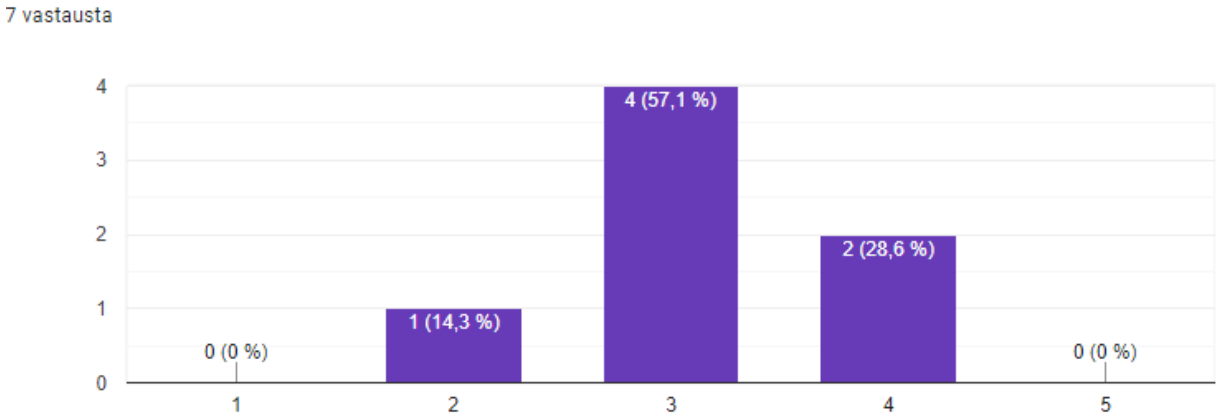
25. Kontrollikanavan häiriösietoisuuden suhteen kontrollikanavat voivat olla joko kaistan sisällä tai kaistan ulkopuolella. Jos kontrolliliikenteelle on varattu kaistan ulkopuolinen ohjauskanava, kognitiivinen radioverkko voi olla pääkäyttäjä (PU = primary user) tällä kanavalla. Siviilimaailmassa tämä on lupaavin tapa välttää häiriöitä muiden käyttäjien kanssa, mutta sotilaallisessa kontekstissa erillinen kontrollikanava muodostaa yhden pisteen vikaantumisen mahdollisuuden (SPoF), joka on alttiina vihamielisen hyökkääjän häirinnälle.



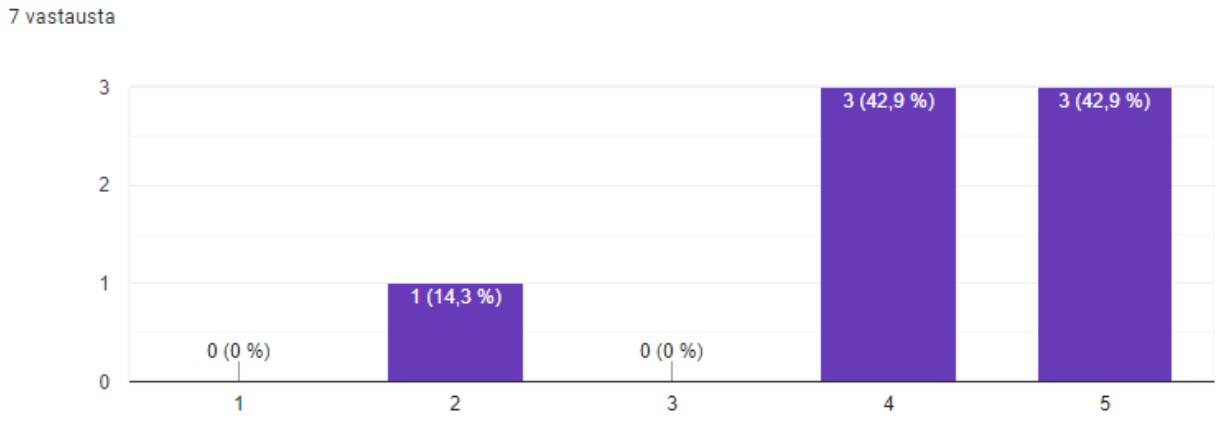
26. Kognitiivisen radioverkon solmut eivät kykene kommunikoimaan ilman toimivaa kontrolliliikennettä. Tietoturvallisuuden näkökulmasta kontrolliliikenteen luottamuksellisuus ja eheys muodostavat uhkan koko verkon toiminnalle.



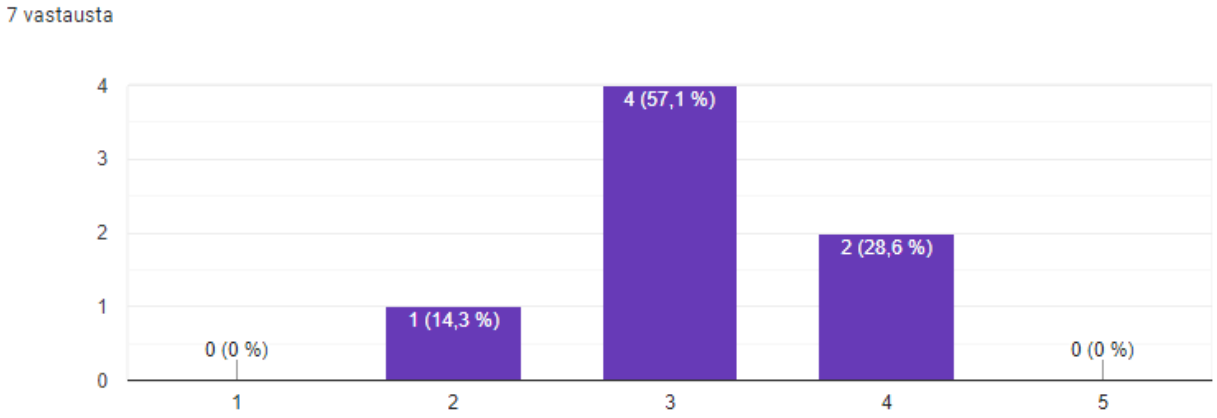
27. Kontrollikanavat voidaan jakaa myös eri verkon osiin (klusteroida). Klusteroitu verkkoarkkitehtuuri voi aiheuttaa liikaa viivettä. Yksi viivettä aiheuttava tekijä on viestien edelleen lähettäminen usean hypyn yli, jos viestin lopullinen vastaanottaja on alkuperäisen lähettimen peittoalueen ulkopuolella. Mitä vähemmän solmuja on suorassa yhteydessä toisiinsa, sitä enemmän viestejä on välitettävä edelleen, mikä kuluttaa edelleen lähettävien solmujen resursseja ja lisää viivettä. Klusteroiduissa verkoissa lisäksi klusterien välinen viestintä johtaa edelleen viiveeseen, koska viestin välittävien yhdyskäytäväsolmujen on vaihdettava lähetystaajuutta.



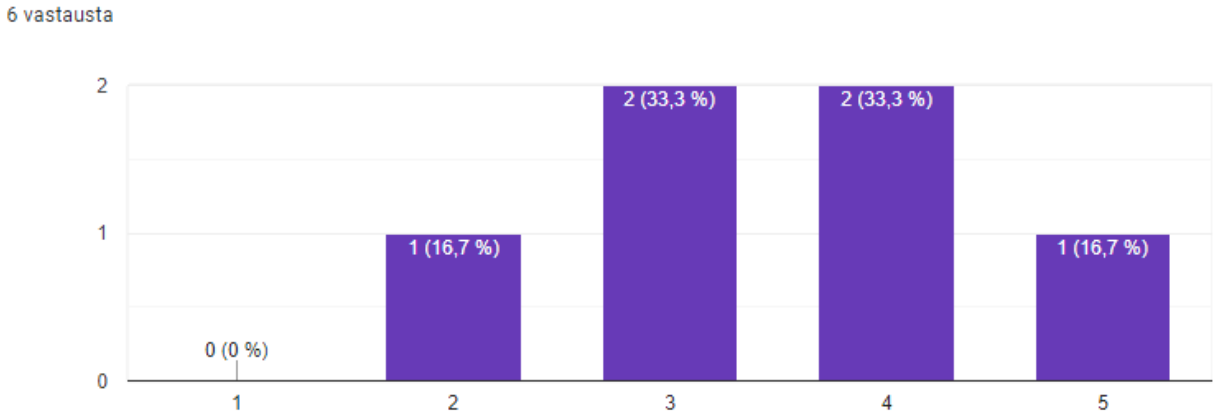
28. Staattinen kontrollikanava edellyttää, että kaikki laitteet käyttävät samoja hyppyparametrejä. Mikäli parametrien toteutus on vuotanut viholliselle, niin vihollinen voi käyttää tätä hyväksi häiritessään yhteyksiä.



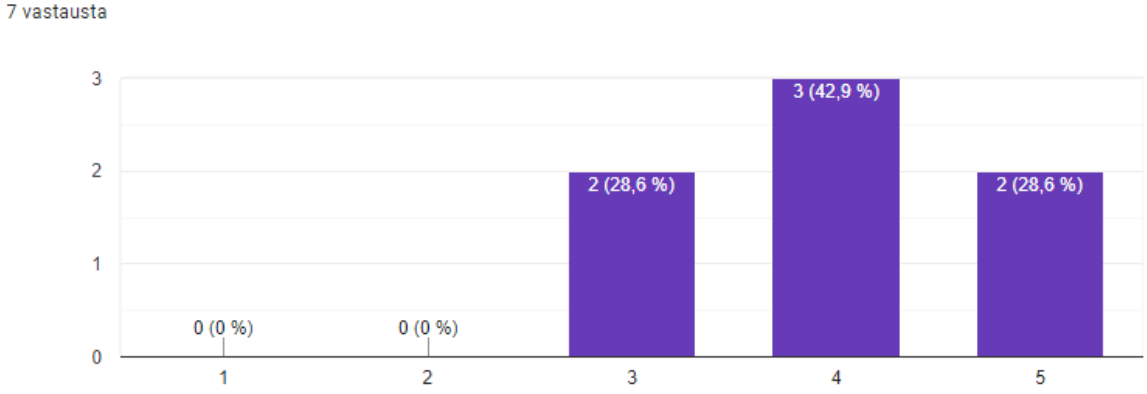
29. Dynaaminen kontrollikanava edellyttää vain, että käytetyt taajuudet tunnetaan. Dynaamisessa kontrollikanavassa solmu tarkkailee yhtä tai useampaa näistä taajuuksista, mikä voi viedä useita aikavälejä (time slot), kunnes lähetin ja vastaanotin ovat löytäneet toisensa. ELSO:sta johtuen voi olla, ettei liikkuvan verkon dynaamisesti muodostuvalla kontrollikanavalla ole tarpeeksi aikaa neuvotella kontrollikanavan muodostumiseksi.



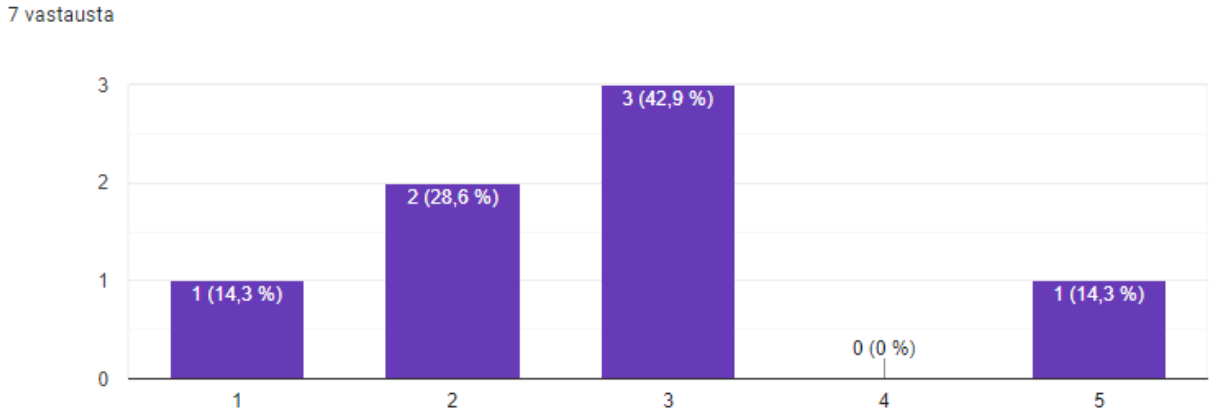
30. Kognitiivisen verkon liiallinen tukeutuminen verkon autonomiseen toimintaan ja sen seurauksena järjestelmän kontrollin menettäminen, tai unohdetaan huolehtia siitä, että verkko todella toimii parhaalla mahdollisella tavalla muodostaa uhkan autonomisessa järjestelmässä.



31. Kognitiiviseen tietoliikenneverkkoon liittyy huomattava määrä ohjelmistollisia parametrejä ja algoritmejä. Näiden suunnittelu, tekeminen, -käsittely, säilyttäminen ja henkilöriskit muodostavat uhkan vihollisen tiedustelun suhteen.



32. Kognitiivinen tekoäly tuottaa jatkuvasti erittäin kattavaa aineistoa. Koko maasta lasketun aineiston tuottama data verkon solmujen sijoitukselle ja niiden tuottamalle suorituskyvylle yhdistettynä alueen operatiiviseen suunnitelmaan muodostaisi korkean tietoturvaluokan materiaalia, joten kokonaisuuden suojaus on mietittävä tarkasti. Myös pienemmät elementit ja niiden tuottama data esim. sotilaallisista harjoituksista operaatioalueen suorituskyvystä tulisi osata luokitella oikeaan tietoturvaluokkaan.



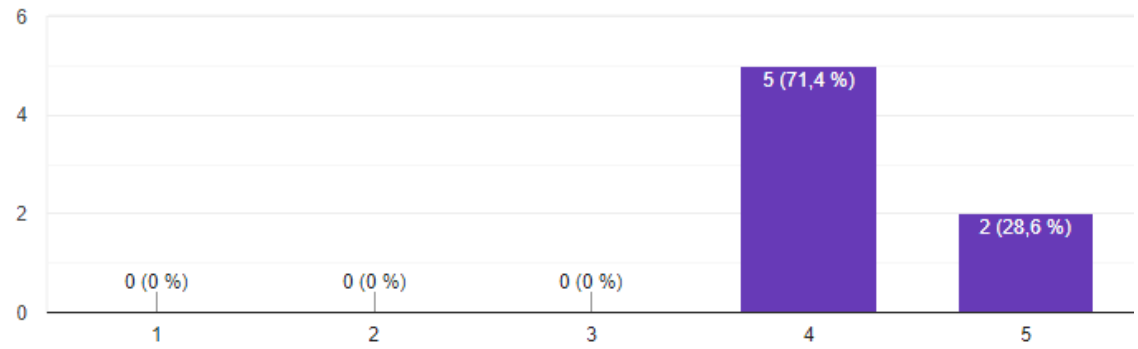
3. Kognitiivisen taktisen tietoliikenneverkon kyberturvallisuutta parantavat toteutusvaihtoehdot

Vastausvaihtoehdot:

	1	2	3	4	5	
Ei merkitystä	○	○	○	○	○	Erittäin suuri merkitys

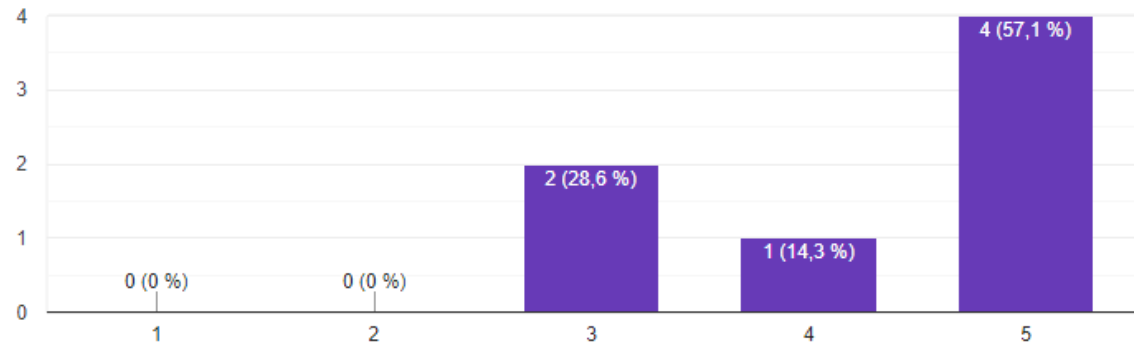
33. Sotilaallisessa ja taktisessa kontekstissa ei saisi muodostua yhden pisteen vikaantumismahdollisuutta (single point of failure, SPoF), jota edustaa SDN:n yksi hallittu arkkitehtuuri. Yhtenä mahdollisuutena on hajautetut arkkitehtuurit, mutta ne aiheuttavat suuren tiedonjakoresurssien tarpeen. SDN-verkon hajautetun ohjauksen hyötyinä ovat sen robusti rakenne ja dynaaminen sopeutuvuus muuttuviin verkkotopologioihin. Se on samalla hyvä häiriösietoisuudeltaan, myös erilaisia kyberhyökkäyksiä vasten. SDN:n hajautettu arkkitehtuuri tulisi ottaa osaksi kognitiivista taktista tietoliikenneverkkoa.

7 vastausta

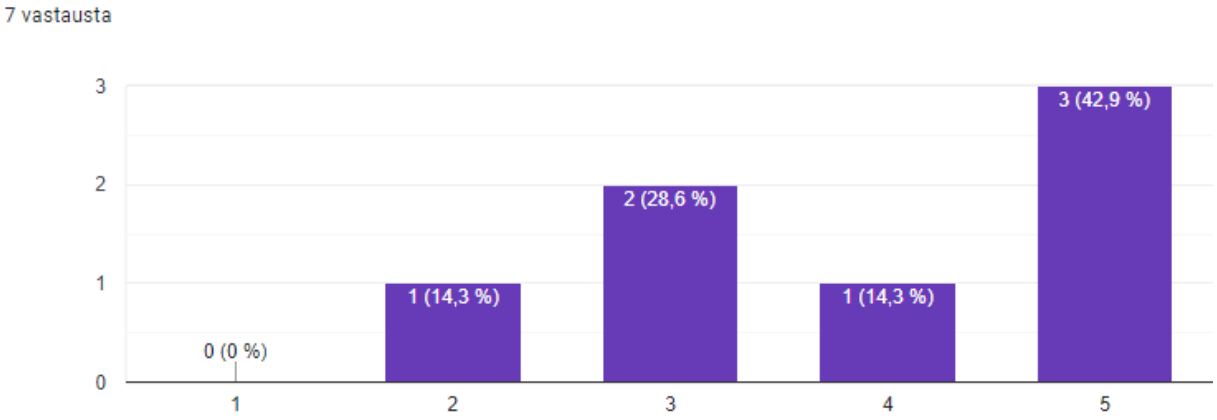


34. Yksittäisen solmun ja verkon tavoitteiden välisten optimointiristiriitojen välttämiseksi tulisi järjestelmässä olla konfliktien purkamisprosessi.

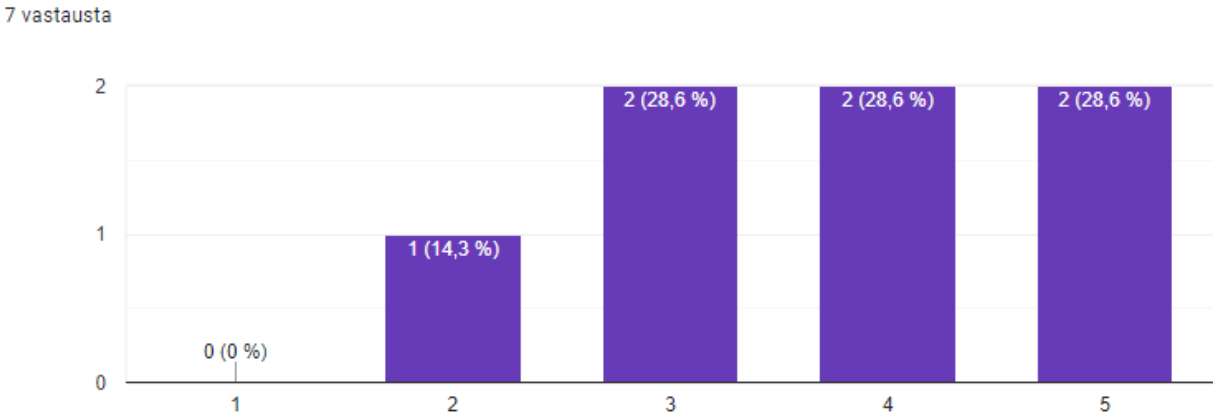
7 vastausta



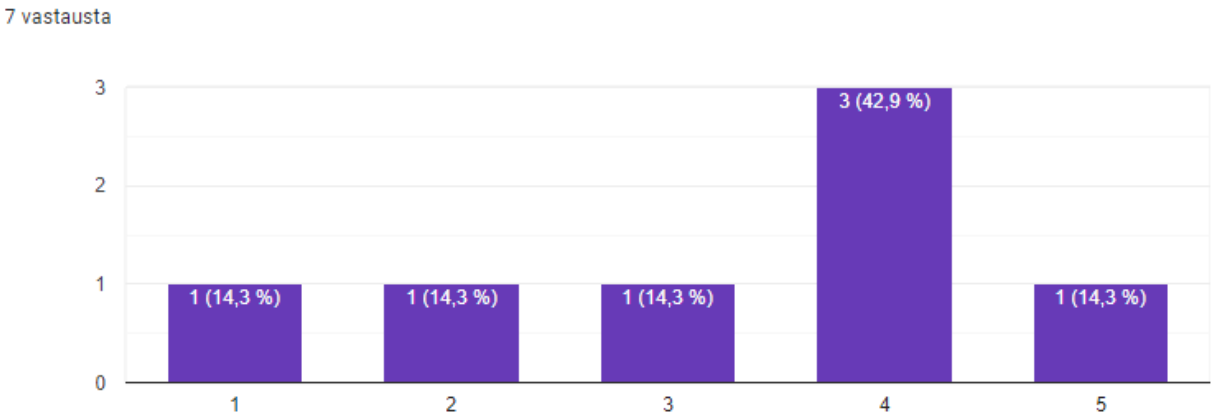
35. Ohjelmisto-ohjattua arkkitehtuuria voidaan käyttää myös hyväksi hyökkäyksiltä suojautumisessa. SDN-verkoissa voidaan hyödyntää esim. reitityssääntöjen asentamista kytkimiin tarvittaessa (reaktiivisesti). Reaktiivista vuosääntöjen luomista voidaan hyödyntää esim. palvelunestohyökkäyksissä.



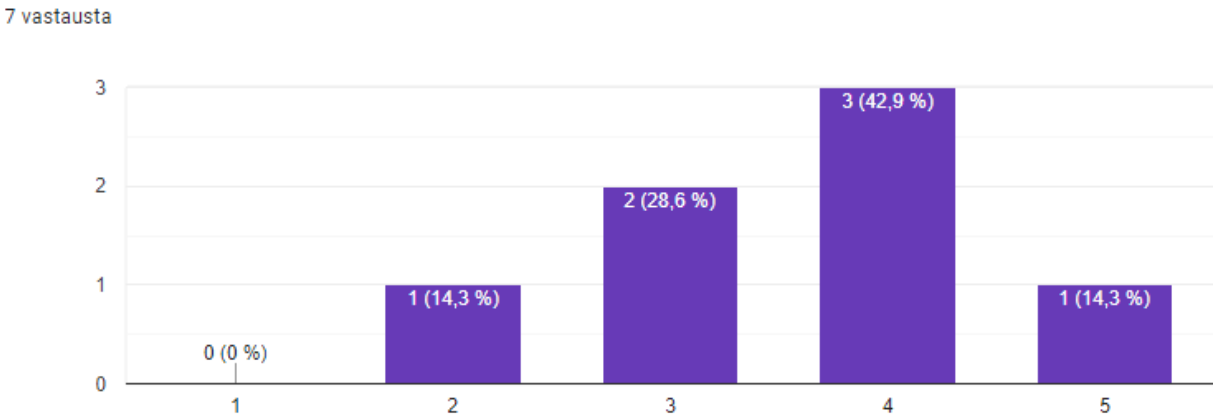
36. Suuri määrä liikennettä SDN-verkossa voi saada kytkimet lähettämään monia paketteja ohjaimelle reitityspäätöstä varten, mikäli niiden reitityssääntöjä ei ole etukäteen lisätty kytkimeen. Tällöin ohjaimen prosessointiteho ei välttämättä riitä, ja liikenne hidastuu kytkinten odottaessa reititysohjeita. Tilannetta voi auttaa ohjaimen hajauttaminen, jolloin kytkimet voidaan jakaa useamman ohjaimen vastuulle.



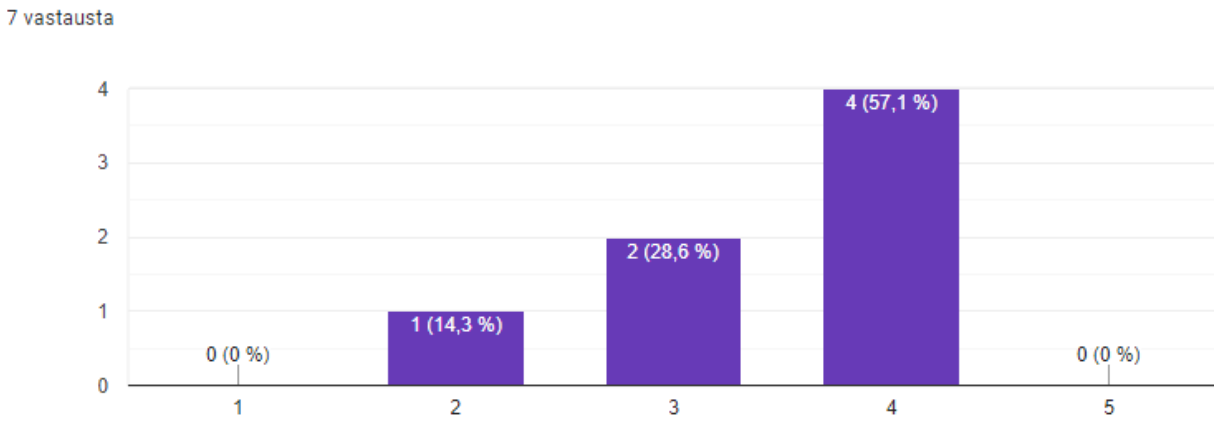
37. Palvelunestohyökkäys voi täyttää kytkimen vuotaulut generoimalla tekaistuja paketteja. Vaikutus perustuu siihen, että ohjain asentaa kytkimeen uuden vuomerkinnän jokaiselle paketille, jonka otsakkeet eroavat edellisistä. Tämä kuluttaa lopulta kytkimen muistin loppuun, eikä uusille vuosäännöille ole enää tilaa. Tällaista hyökkäystä vastaan on ehdotettu kahta ratkaisua: joko ohjaimen pitäisi pystyä pitämään verkko toiminnassa kytkimen muistin loppumisesta huolimatta, tai ohjain voisi väliaikaisesti tallentaa vuomerkintöjä itse ja vaihtaa niitä kytkimeen tarpeen mukaan. Muun muassa suositun OpenFlow-protokollan määritelmä sallii kytkinten poistaa vuosääntöjä itsenäisesti.



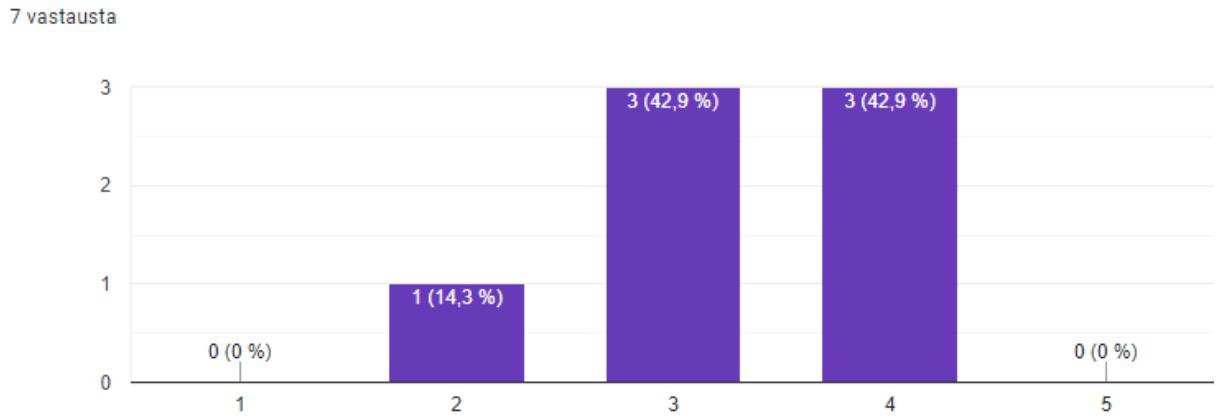
38. Mahdollinen puolustuksellinen vastatoimenpide voisi olla palvelunestoliikenteen dynaaminen ohjaus esimerkiksi niin sanottuun hunajapurkkiin hyökkäyksen analysoimiseksi.



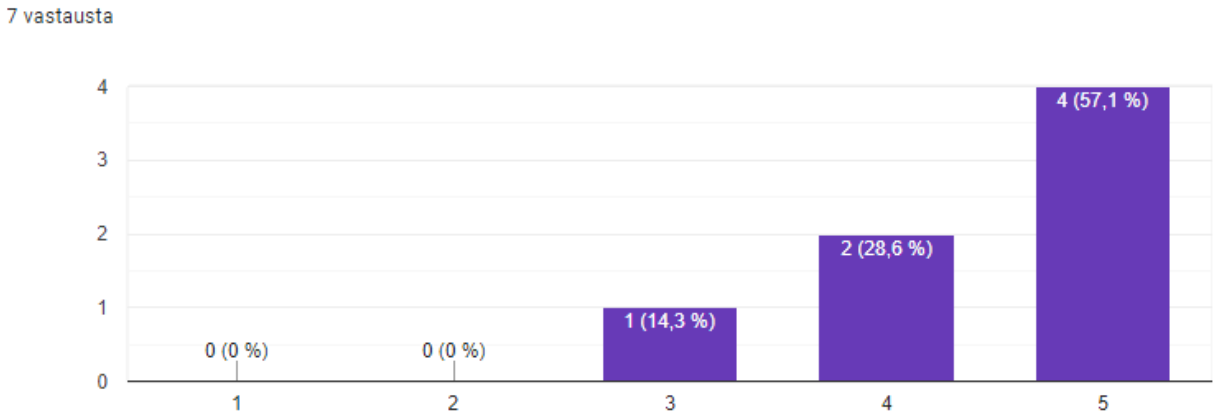
39. OpenFlow-toteutuksen edeltäjässä, Ethane-arkkitehtuurissa on loogisesti keskitetty ohjain, joka hallitsee yksinkertaisia kytkimiä. Tietoturvallisuus on toteutettu kiinteänä osana arkkitehtuuria esimerkiksi pääsynhallinnan muodossa. Ethane myös sitoo paketin ja sen lähettäjän tiukasti yhteen, jolloin käyttäjien seuraaminen on mahdollista, vaikka sijainnit muuttuisivatkin. Ohjelmisto-ohjatussa tietoverkossa turvallisuutta ei ole suunniteltu kiinteäksi osaksi arkkitehtuuria, joten Ethanen tietoturvan toteutuksesta voitaisiin ottaa oppia ohjelmisto-ohjattuihin tietoverkkoarkkitehtuureihin.



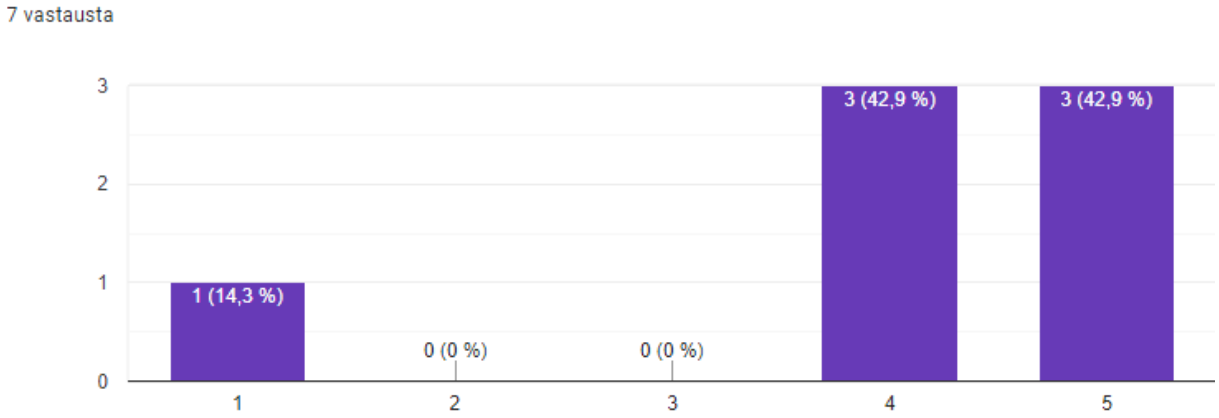
40. Ohjelmisto-ohjattu tietoturvallisuus (SDSec, Software-Defined Security) parantaisi kognitiivisen tietoliikenneverkon turvallisuutta erityisesti pääsynhallinan ja autentikoinnin suhteen.



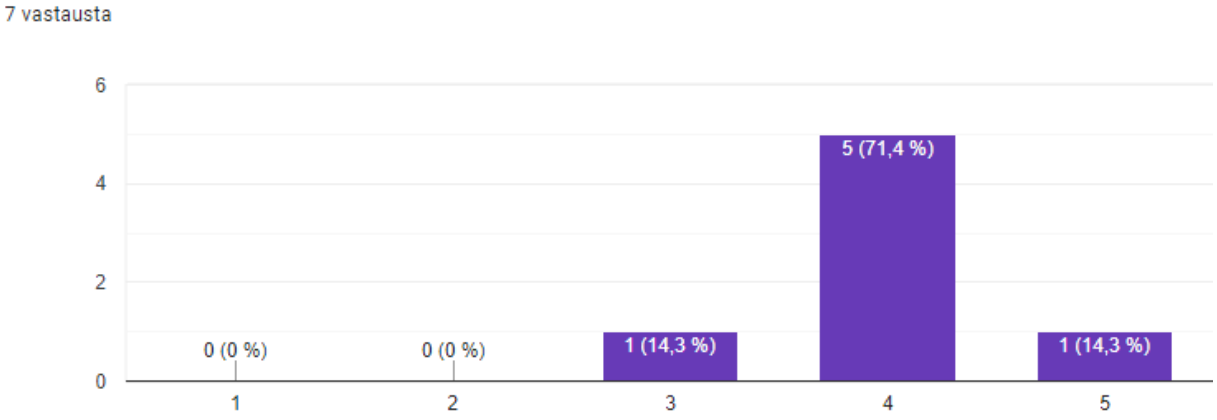
41. Verkkotoimintojen virtualisoinnilla (Netvork Function Virtualization, NFV) tarkoitetaan verkkotoimintojen toteutusta ohjelmallisesti yleisillä ja kaupallisesti saatavilla olevilla tietojenkäsittelykomponenteilla. Virtualisoituja verkkotoimintoja voivat olla esimerkiksi liikennekuorman tasaaminen, palomuurit ja tunkeutumisen havaitsemisjärjestelmät (Intrusion Detection/Prevention System, IDS/IPS). Virtualisoidut verkkotoiminnot arkkitehtuuriratkaisuna eivät ole riippuvaisia ohjelmisto-ohjatusta tietoverkosta, vaan niitä voidaan toteuttaa itsenäisesti jo nykyisiä verkko- ja hallintaperiaatteita hyödyntäen. Ohjelmisto-ohjaus (SDN) yhdessä verkkovirtualisoinnin (NFV) kanssa helpottaa verkkojen dynaamista resurssien hallintaa sekä palvelujen ohjausta. Näiden molempien lähestymistapojen yhdistelmällä voidaankin saavuttaa etuja hallinnan ja operoinnin suhteen.



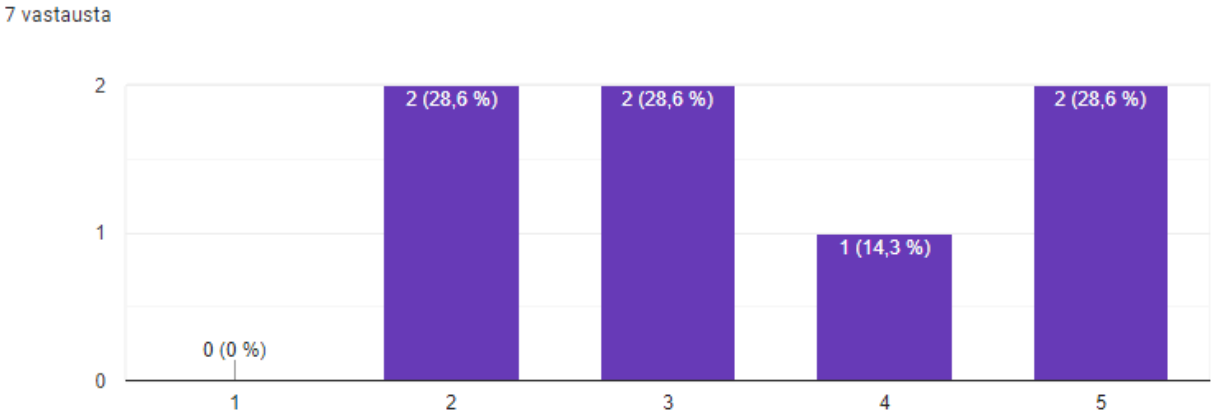
42. Ohjelmisto-ohjatun verkon tietoturva on perinteistä tietoverkkoa helpompi pitää ajan tasalla päivittämällä sovelluksia sen sijaan, että vaihdettaisiin fyysisiä verkkolaitteita tai päivitettäisiin niitä yksittäin. Lisäksi arkkitehtuurissa uusien ominaisuuksien toteuttaminen on nopeampaa.



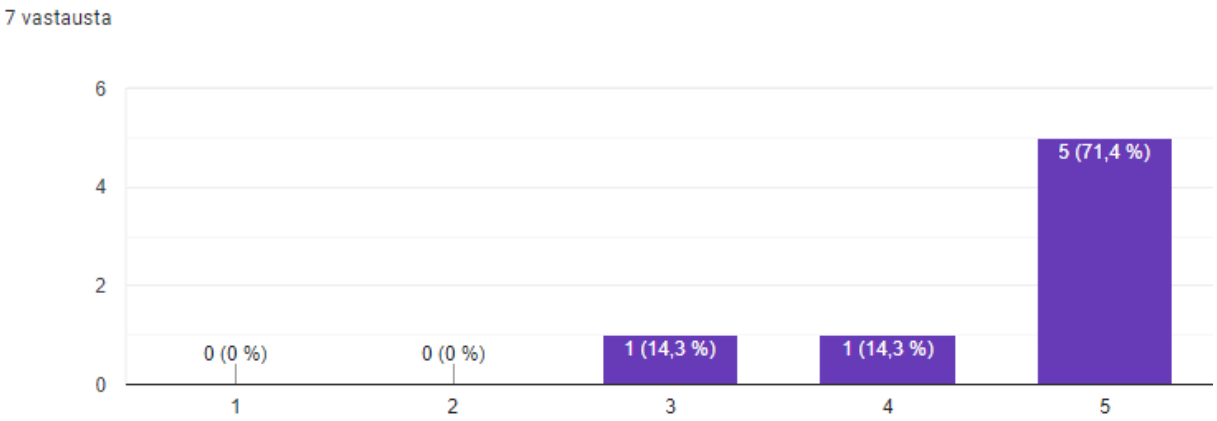
43. Klusterointi on tärkeää robustin verkon suunnittelussa. Klusteroinnin tulisi siksi tukea myös muita taktisissa kognitiivisissa radioverkoissa käytettyjä tekniikoita.



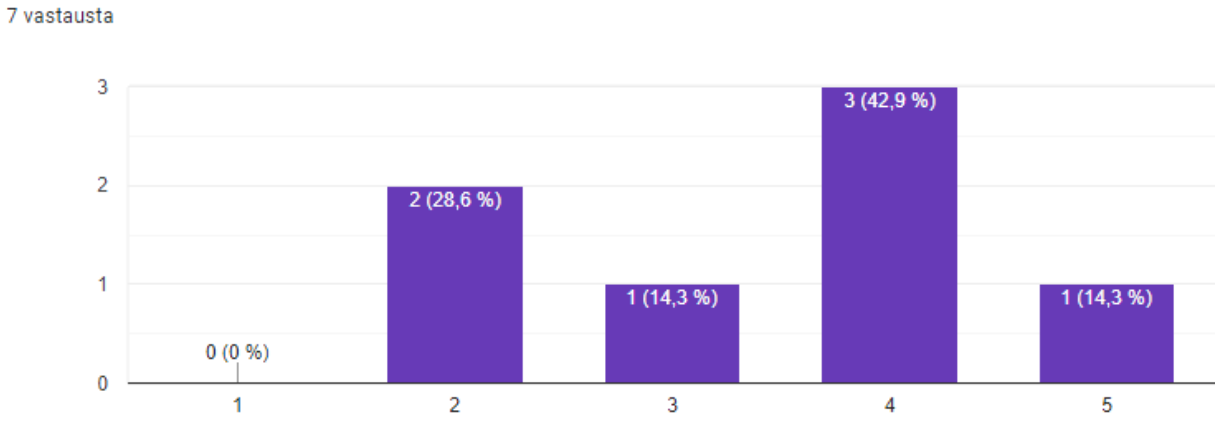
44. Kontrollikanavan on käsiteltävä voimakkaasti vaihtelevaa tietoliikennemäärää, minkä vuoksi sen tulisi olla mukautettavissa sen hetkiseen liikennemäärään.



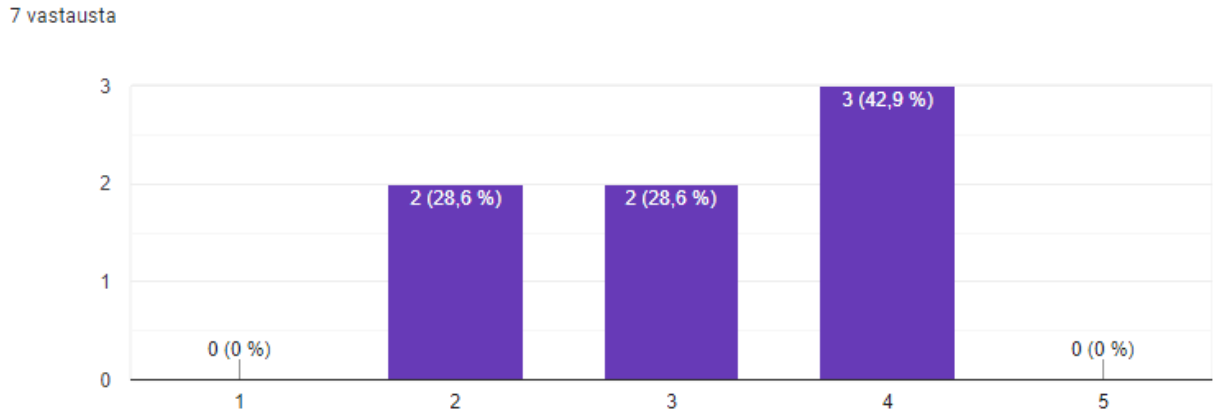
45. Häirintäjärjestelmien käytössä kognitiivisia radioita vastaan voidaan spektriin luoda tilanteita, joihin kognitiivisen radion halutaan reagoivan halutulla tavalla. Suojautumisen näkökulmasta näihin erilaisiin tilanteisiin tulee varautua etukäteen simuloimalla ja mallintamalla häirintä- ja häiriöskenaarioiden vaikutuksia kognitiivisen radion eri toimintatapamalleissa.



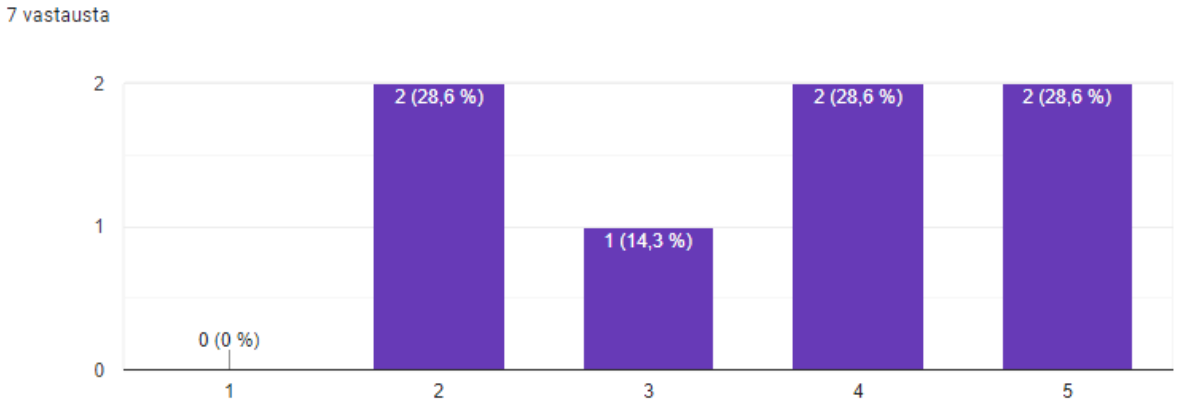
46. Verkon kontrolliliikenteen suhteen kaikkien viestien lähettämisen on tapahduttava tarvittaessa samanaikaisesti ja ne on varustettava eri prioriteeteilla verkon kaikissa solmuissa. On varmistuttava, että kaikki viestit voidaan toimittaa ajoissa, mistä syystä kontrollikanavalla on oltava riittävät resurssit liikenteen tukkeutumisen välttämiseksi.



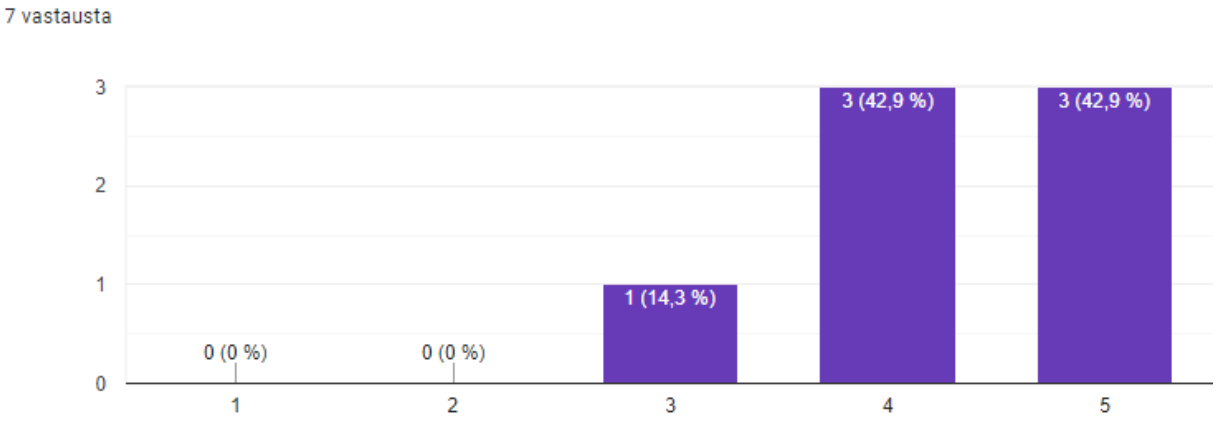
47. Yksi ratkaisu häirinnän väistöprosessiin liittyen on sellaisten signaalien lähettäminen, joilla on hyvät korrellaatio-ominaisuudet (voidaan havaita häiriöistä huolimatta). Käytettäessä CDMA-koodijakokanavointia ennalta määriteltyjen jakokoodien kanssa, erilaisten ilmoitusten vastaanottaminen on mahdollista.



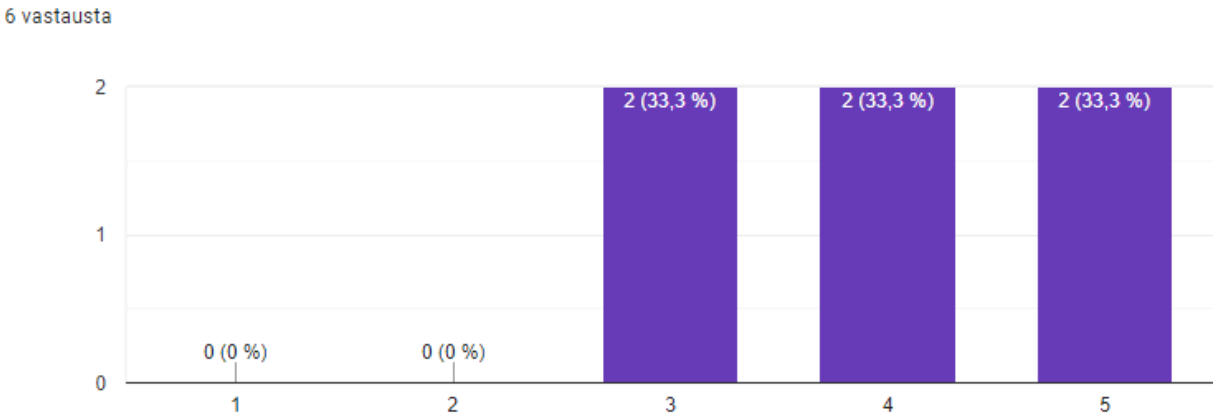
48. Mikäli solmulla on käytettävissä kaksi radioetupäätä, häirityn kanavan väistöstä voidaan antaa ilmoitus toisen radioetupään kautta vapaalla kanavalla.



49. Kognitiivisen verkon taajuushavainnointitietojen väärentämisuhkaan on esitetty lukuisia solmujen luottamuksen arviointiin perustuvia tekniikoita, joiden tehtävänä on tunnistaa haitalliset solmut ja estää näiden välittämät virheelliset tiedot. Järjestelmän kognitiivisten päätösten luottamusaste voidaan arvioida suorien vuorovaikutusten, havaintojen ja suositusten perusteella. Solmut vaihtavat keskenään signalointiviestejä, joita tarvitaan tietämyksen lisäämiseksi spektriympäristöstä (ts. havaintopohjainen) tai tukemaan dynaamista taajuuksien käyttöoikeutta ja hallintaa (ts. kognitiivinen reititys, topologian hallinta). Jos todennetun solmun kognitiivinen moottori yrittää lähettää vääriä tietoja (esimerkiksi havaintojen tuloksista), muu verkko voi romahtaa kokonaan. Tästä syystä solmujen tuottama tieto tulee olla luotettavaa. Luotetut ja epäluotetut solmut tulee ottaa huomioon reititysvalinnassa, ja epäluotetut solmut tulee kyetä poissulkemaan järjestelmässä. Siksi solmujen luotettavuuden arviointitekniikat tulisi olla kiinteänä osana kognitiivista tietoliikenneverkkoa.

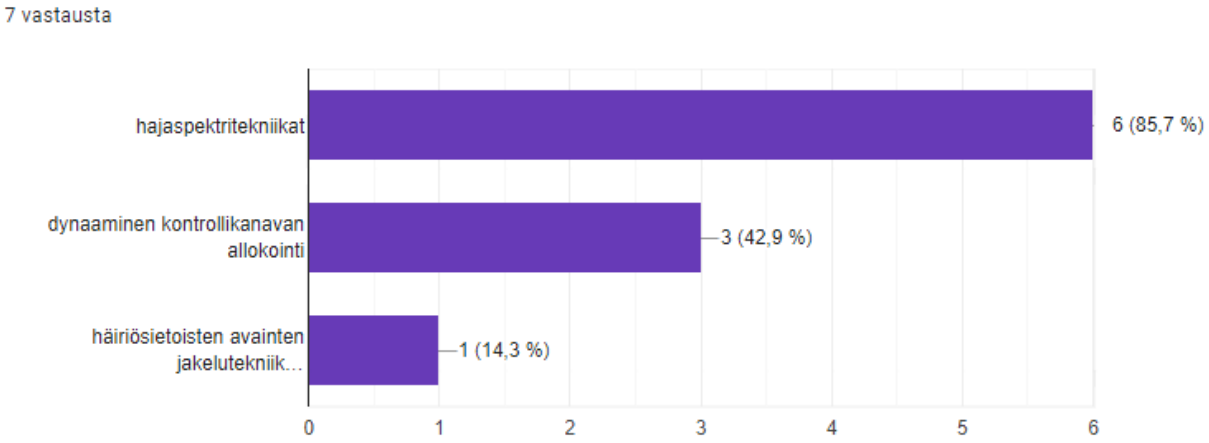


50. Kognitiivisen verkon parametrejä suunnitellessa tulisi huomioida, miten välttää verkon toiminnan perusteella vihollisen häirinnän tehoamisen paljastuminen.

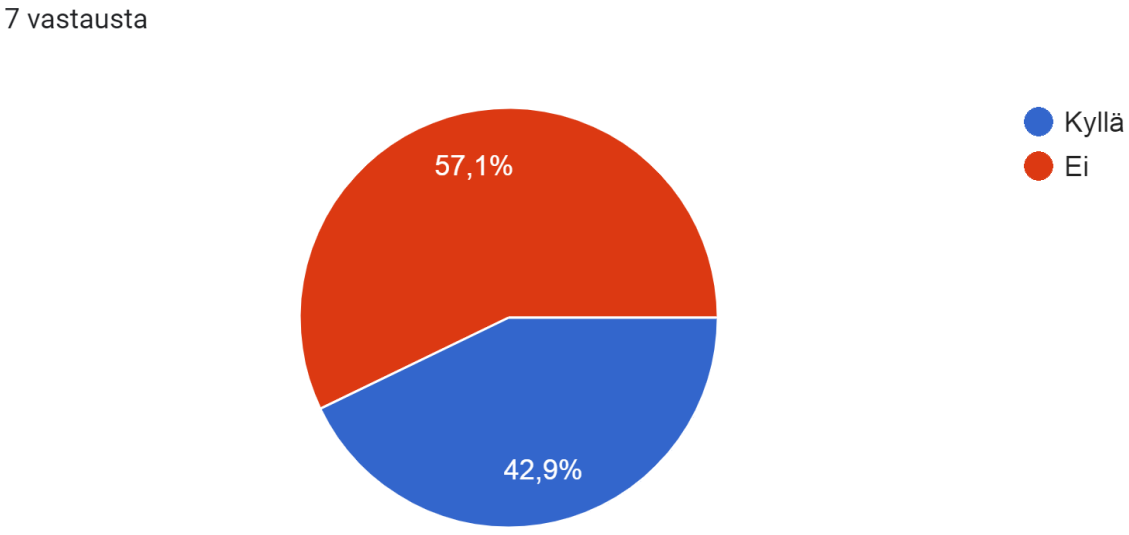


Monivalintakysymykset

51. Yhden pisteen haavoittuvuuksien välttäminen kontrolliliikenteessä on kriittisen tärkeää kognitiiviselle radioverkolle. Mitkä näistä tekniikoista olisi tärkeitä tämän haavoittuvuuden turvaamiseksi?

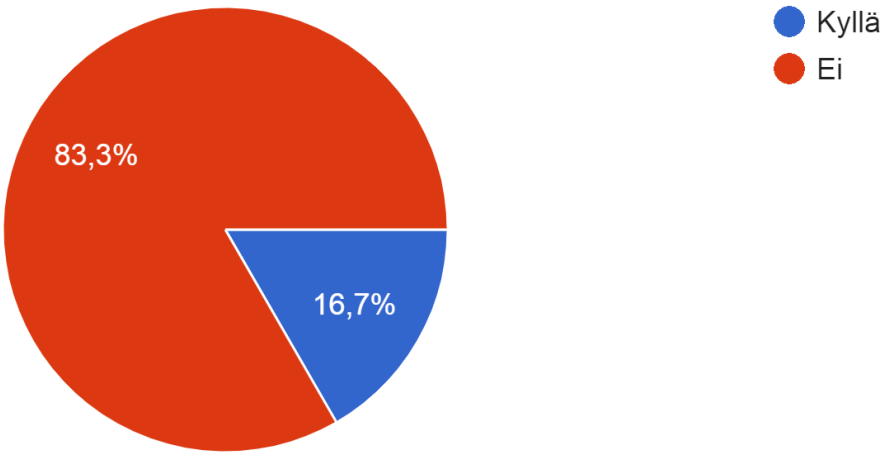


52. Etäisyyden hyödyntämiseksi ensisijaisen käyttäjän tunnistamiseksi esitetään kahta tekniikkaa ongelmien ratkaisemiseksi. Ensimmäistä tekniikkaa kutsutaan etäisyyssuhteeksi (DRT, distance ratio test), joka käyttää vastaanotetun signaalinvoimakkuuden (RSS, received signal strength) mittaustuloksia, jotka on saatu sijaintitodentajilta (LV, location verifiers) lähettimen sijainnin varmistamiseksi. Sijaintitodentaja voi olla erillinen verkkolaite tai toisiokäyttäjä, jolla on tehostetut toiminnot paikannustarkistuksen suorittamiseksi. Jos odotettu RSS-arvo ja mitattu RSS-arvo ovat riittävän lähellä (ennalta määrättyyn tarkkuuteen), lähetin läpäisee sijaintitestin ja todetaan ensisijaiseksi käyttäjäksi. DRT-tekniikan toimivuuteen vaikuttaa kuitenkin tosiasiallinen radioaallon etenemismalli, johon puolestaan vaikuttavat erilaiset ympäristömuuttujat. Olisiko em. tekniikka mielestäsi käyttökelpoinen taktisessa kognitiivisessa verkossa?



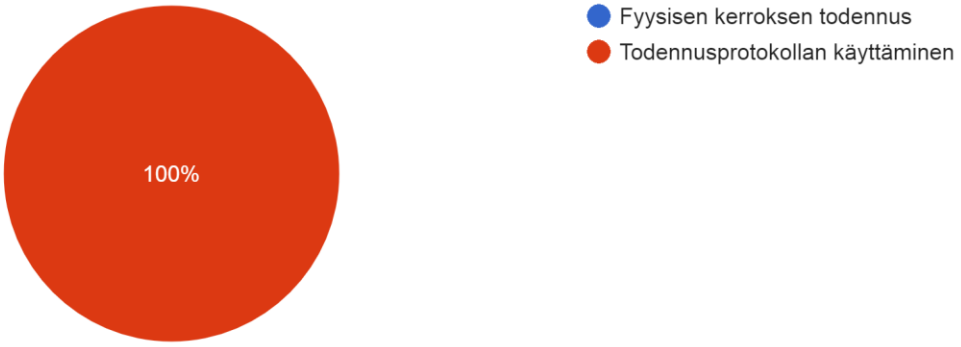
53. Etäisyyden hyödyntämiseksi ensisijaisen käyttäjän tunnistamiseksi esitetään kahta tekniikkaa ongelmien ratkaisemiseksi. Toista tekniikkaa kutsutaan etäisyyserotestiksi (DDT, distance difference test). Tämä tekniikka hyödyntää signaalin vaihe-eroa. Kun signaali lähetetään yhdestä lähteestä kahteen LV:iin, voidaan havaita suhteellinen vaihe-ero johtuen niiden etäisyydestä lähettimen suhteen. Vaihe-ero voidaan taas muuntaa aikaeroksi, joka puolestaan voidaan muuntaa etäisyyseroksi. Täten voidaan laskea kunkin LV:n ja lähettimen oletettujen keskinäisten etäisyyksien ero käyttämällä kahden LV:n sijaintitietoja ja ensisijaisen lähettimen oletettua sijaintia. Tätä oletettua eroa verrataan mitattuun eroon ensisijaisen käyttäjän signaalin aitouden määrittämiseksi. Jos nämä kaksi arvoa ovat riittävän lähellä, lähetintä pidetään ensisijaisena käyttäjänä. Vaikka DDT ei kärsi DRT:n haitoista, DDT vaatii LV:ien välillä tehokasta synkronointia (satojen nanosekuntien luokkaa), jonka toteuttaminen voi olla kallista. Olisiko em. tekniikka mielestäsi käyttökelpoinen taktisessa kognitiivisessa verkossa?

6 vastausta



54. Ensisijaisen käyttäjän emulointihyökkäyksiä varten tulisi olla tekniikka ensisijaisen käyttäjän signaalin aitouden todentamiseksi. Yksi mahdollinen lähestymistapa on käyttää signaalin todentamista fyysisessä kerroksessa käyttämällä RF-signaalin ominaisuuksia, jotka liitetään tietyn lähettimen tai lähettimien ominaisuuksiin, tai yksinkertaisesti lisäämällä varmenteita ensisijaisen käyttäjän signaaliin. Fyysisen kerroksen todennuksella vältetään ylemmän kerroksen todennukseen liittyvät otsikkotiedot, mutta se voi olla vähemmän luotettava, koska ominaisuudet tai varmenteet ovat signaalin heikkenemisen kohteena. Toinen menetelmä on käyttää todennusprotokollaa ensisijaisen käyttäjän lähettimen ja todentajan välillä. Kumpi näistä olisi mielestäsi parempi ratkaisu?

6 vastausta

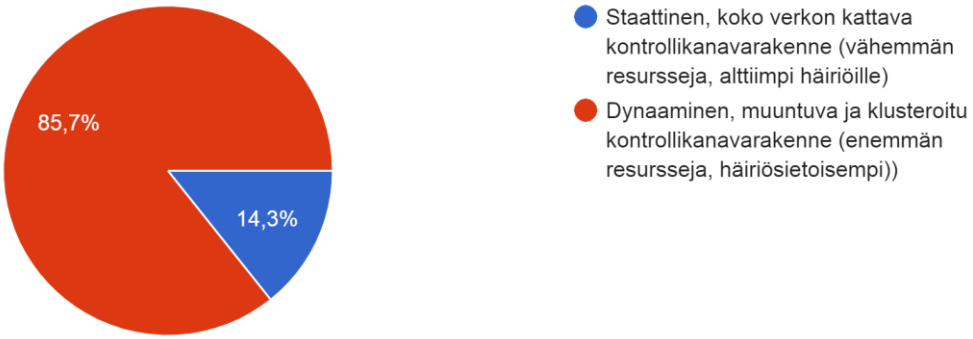


55. Kaistan ulkopuolisen kontrollikanavan tekninen toteuttaminen vaatii joko radioetupään (RHU, radio head unit) erityisen nopean taajuudenvaihdon (taajuushypintä) tai vaihtoehtoisesti tarvitaan enemmän kuin yksi radiopää, mikä voi johtaa yhteisvaikutuksiin. Kumpi näistä olisi mielestäsi parempi ratkaisu häiriösietoisuuden suhteen?

6 vastausta

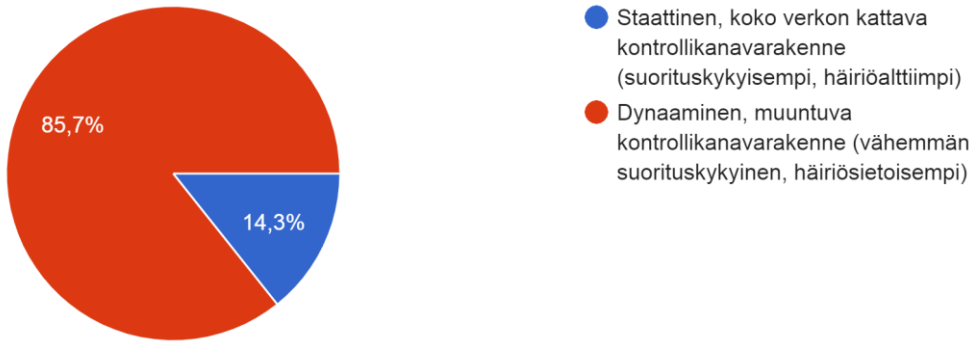
56. Kontrollikanava voi olla melko staattinen ja siten tarjota ennalta suunnitellun kattavuuden kaikille solmuille, tai se voi olla dynaaminen ja yhdistää vain muutaman solmun pyynnöstä. Klusteroinnin avulla verkko voidaan jakaa useisiin aliverkkoihin käyttämällä erilaisia kontrollikanavia. Vaatimuksena on kuitenkin, että kaikkien solmujen välillä on oltava mahdollista vaihtaa kontrollitietoja. Vaikka staattinen kontrollikanava on altis häiriöille, dynaaminen ohjauskanava vaatii enemmän resursseja yhteyksien muodostamiseksi. Kumpi mielestäsi olisi parempi ratkaisu kontrollikanavan toteutukselle?

7 vastausta



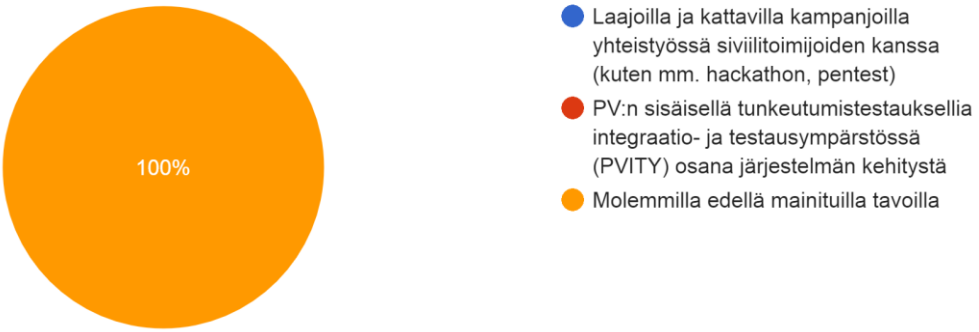
57. Kuva osoittaa, että staattinen tai dynaaminen kontrollikanava on kompromissi suorituskyvyn, joustavuuden ja kontrolliliikenteen kyllästymisen suhteen. Vaikka dynaaminen kontrollikanava voi joustavasti mukautua tiedonvaihtotarpeisiin ja välttää siten liikenteen kyllästymistä, neuvottelut kontrollikanavan muodostamisesta heikentävät suorituskykyä. Puhtaasti staattiset kontrollikanavat eivät tarvitse tällaisia neuvotteluja, mutta toisaalta eivät voi myöskään sopeutua vaihtelevaan kontrollitietojen vaihtoon. Kumpi olisi mielestäsi parempi toteutusvaihtoehto taktisen kognitiivisen radioverkon kontrollikanavan rakenteen suhteen?

7 vastausta



58. Kognitiivisen taktisen tietoliikennejärjestelmän kyberturvallisuutta tulisi testata hyökkäämällä sitä vastaan.

7 vastausta

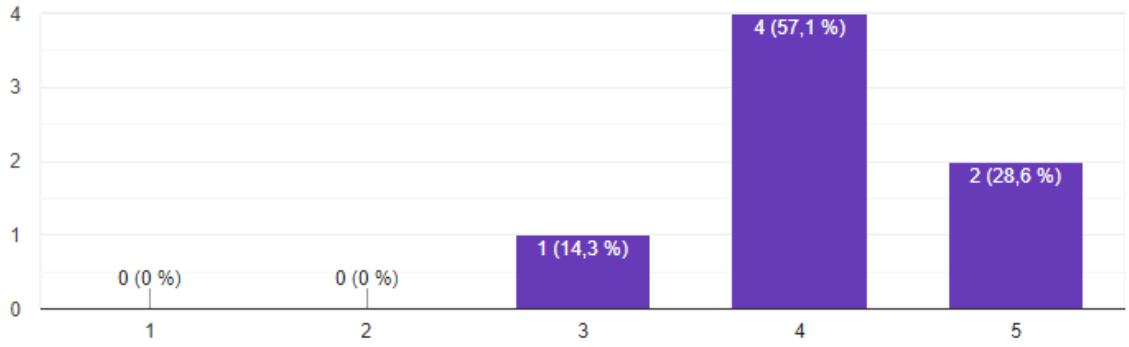


4. Kognitiivisen taktisen verkon muut vaatimukset

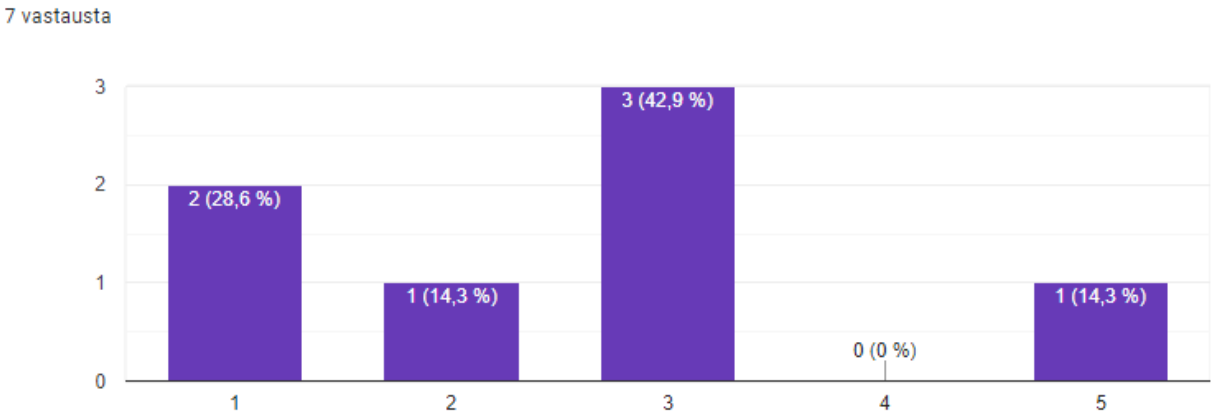
Vastausvaihtoehdot:

59. Kognitiivisuus automatisoi verkon suunnittelua ja hallintaa ja luo mahdollisuuksia johtamisjärjestelmien automaattisen suunnittelun ja hallinnan helpottamiseksi operaatioiden toimeenpanemisessa. Kognitiivisen taktisen tietoliikenneverkon tulisi kyetä automaattisesti suunnittelemaan verkkorakenteensa.

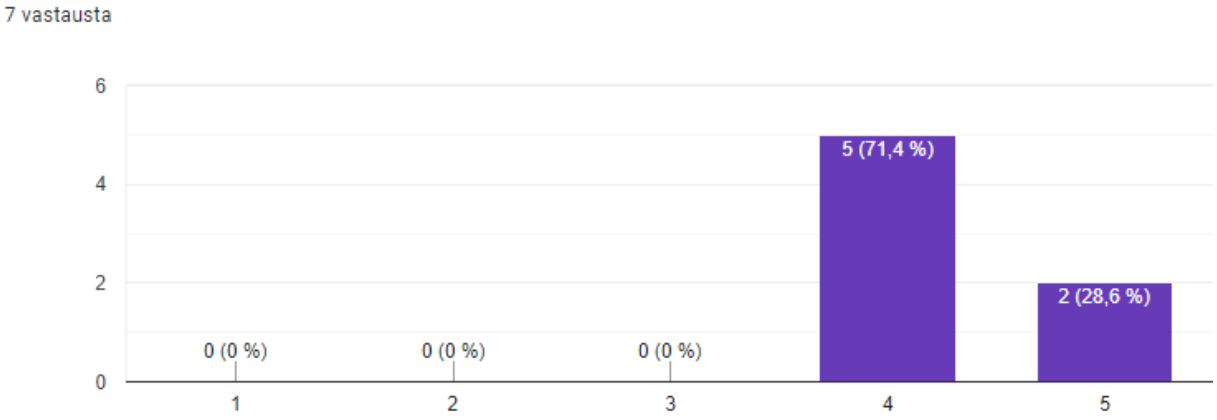
7 vastausta



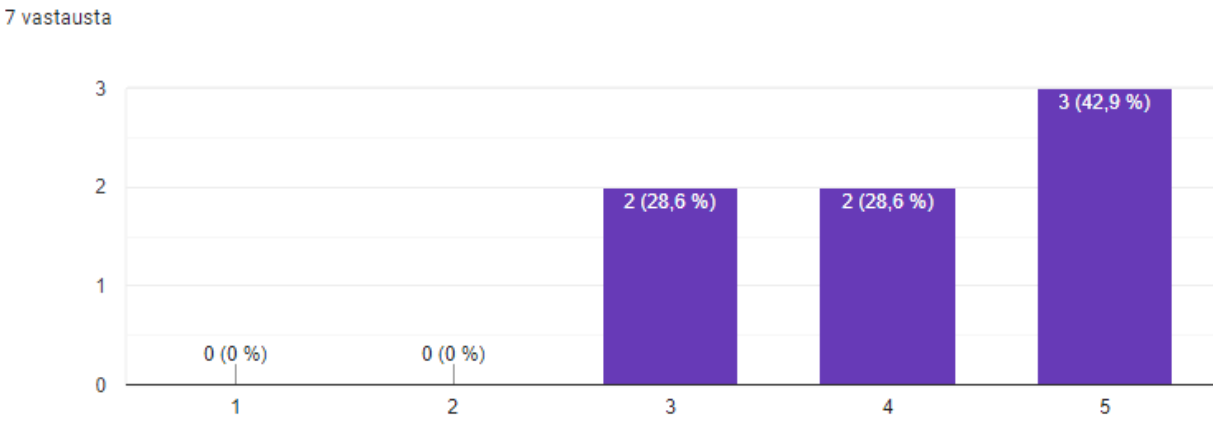
60. Kognitiivisen taktisen verkon suunnitteluperusteet tulee edelleen luoda manuaalisesti.



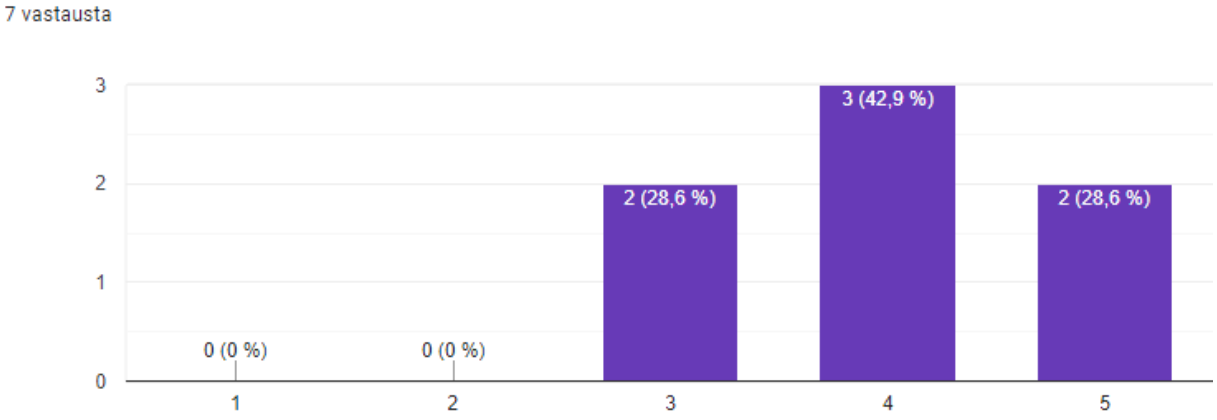
61. Kognitiivista verkkoa ja sen toimintaa / toiminnallisuuksia tulee kyetä valvoa ja hallita ihmisen toimesta. Kognitiivisessa verkossa tulisi olla mahdollisuus manuaaliohjaukseen protokollien ja yhteydenmuodostuksen saralla, sekä käyttäjän mahdollisuus poistaa yhteyksiä / toiminnallisuuksia.



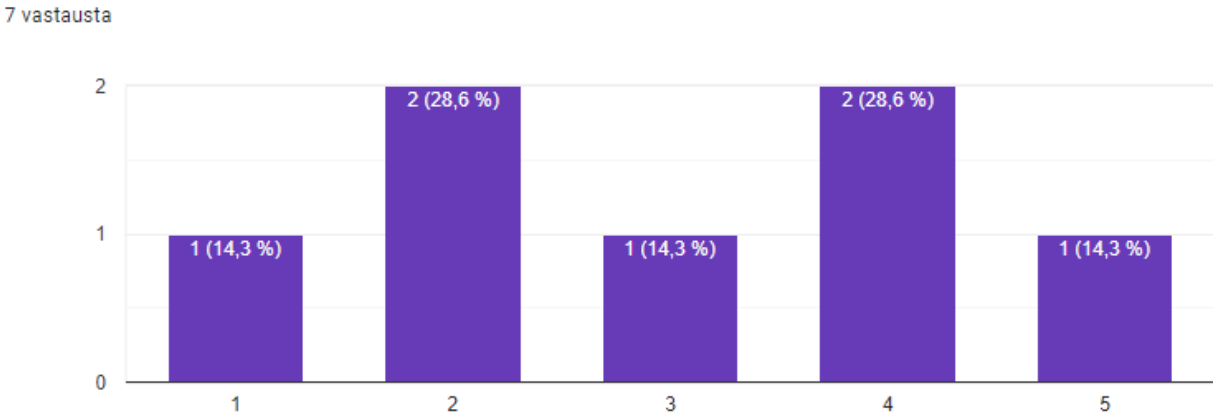
62. Kognitiivisen verkon adaptiivisuuden ja optimoinnin suhteen tehtävän ja operaation suoritusvaiheen tulisi vaikuttaa haluttuun lopputulokseen (tilannekuva, salaaminen, harhauttaminen, tiedustelu, tulenjohto, häirinnän väistö, kokonaissuorituskyky).



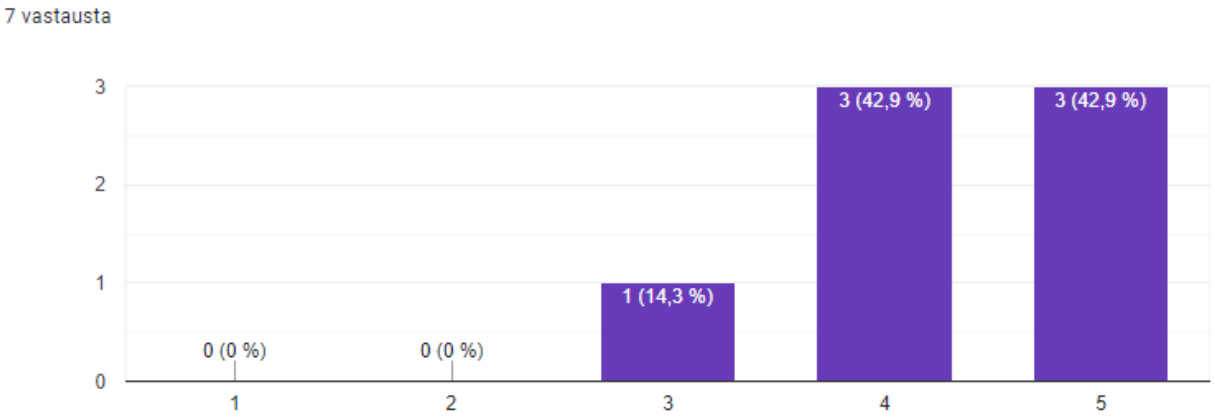
63. Kognitiivisilla radioilla tulee olla kyky toimia ELSO-sensoreina ja häirintälähettiminä tarvittaessa.



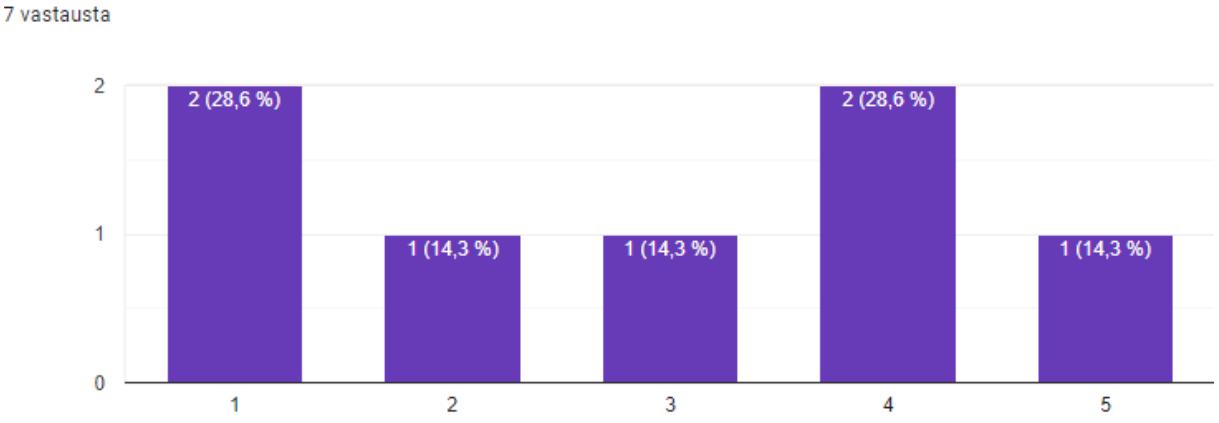
64. Kognitiivisilla radioilla tulee olla kyky häirintälähettimenä toimiessaan lähettää viholliselle autenttisen oloista liikennettä.



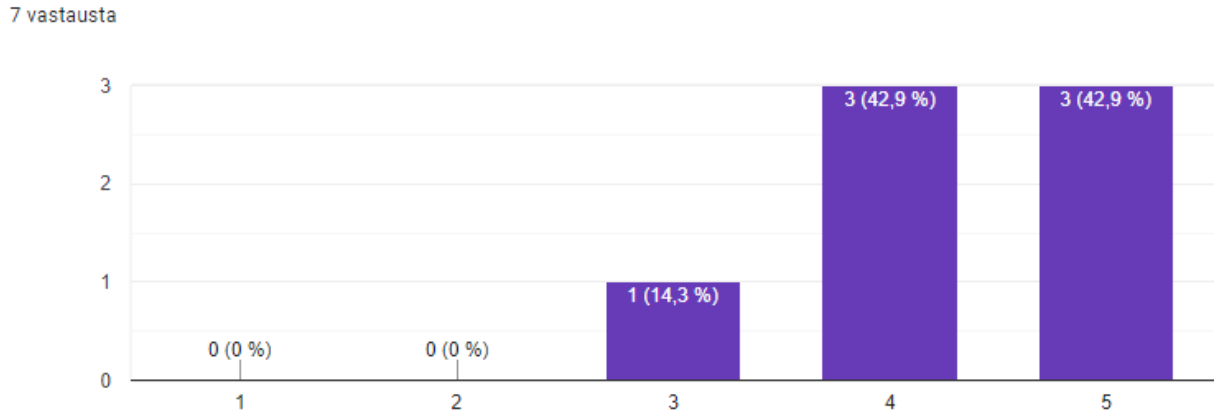
65. Taajuus-spektrin suhteen antennien sekä radion olisi kyettävä hyödyntämään mahdollisimman laajaa taajuuskaistaa (UHF, VHF, HF).



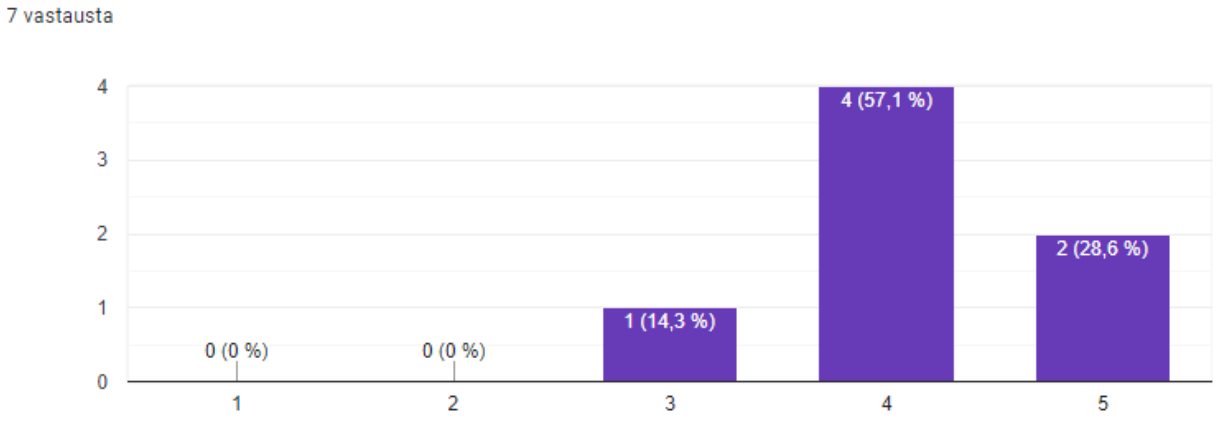
66. Kognitiiviseen radioverkkoon tulisi kyetä lisäämään myös vanhemman sukupolven ei-kognitiivisia ohjelmistoradioita, joille kognitio voi antaa rajattuja ohjauskomentoja ja asettaa rajoitetusti tiedonsiirtoparametreja.



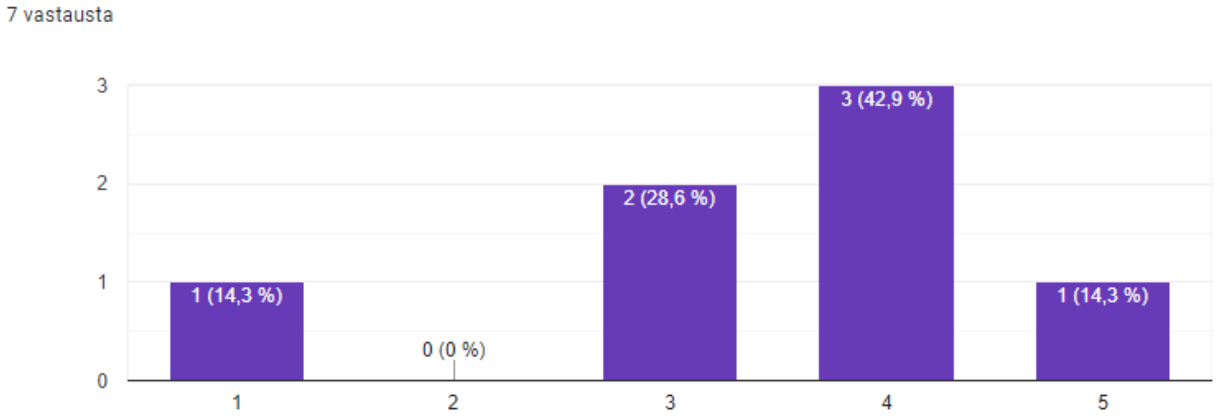
67. Laajasta taajuus-spektristä johtuen antenneja tulee olla useanlaisia, ja osa niistä olisi suunta-antenneja. Kognitiivisella radiolla tulisi olla kyky ohjata radion antenneja.



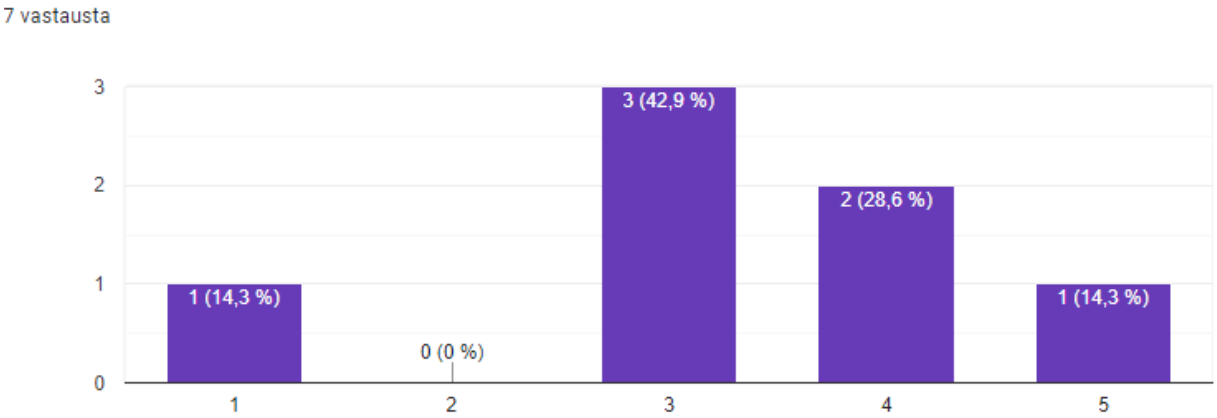
68. Esimerkiksi älykkäiden SBA-tyyppisten antennien avulla voitaisi parantaa merkittävästi verkon palvelukykyä. Samoin automaattisesti radiosta ohjatut aktiiviantennit optimoivat verkkoa radioiden hypintä- ja taajuus-suunnitelman mukaiseksi vähentäen havaittavuutta ja parhaimmillaan kaksinkertaistaen linkkipituudet.



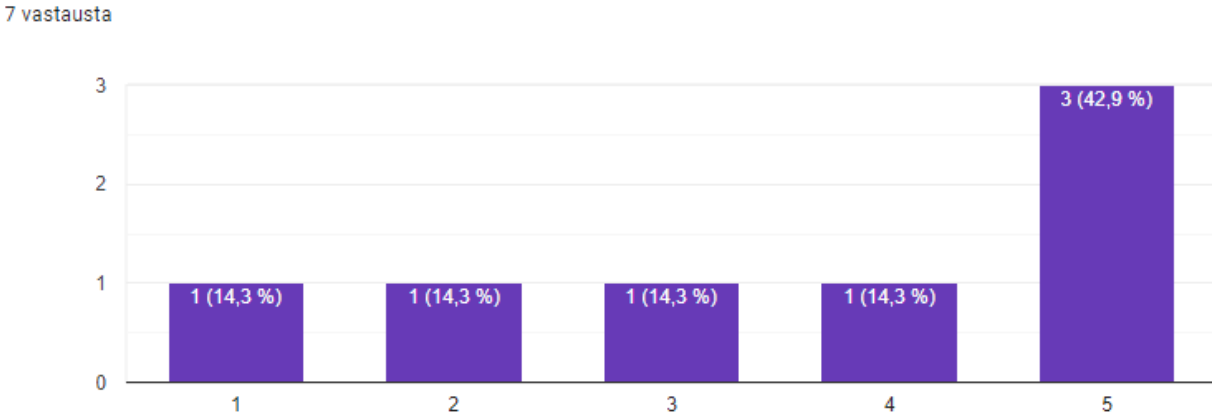
69. Suunta-antenneilla vastustajan ELSO-vaikuttaminen voidaan helposti havaita hypyttämällä vastaanotinta koko taajuusalueella ja samanaikaisesti pyörittämällä sähköisesti keilattavaa antennia, jolloin aseman ympäriltä havaitaan 360-asteen leveydeltä tapahtuva mahdollinen vaikuttaminen. Tieto voidaan käsitellä tekoälyllä ja koko järjestelmä suojata kieltämällä vastaanotto ko. suunnista.



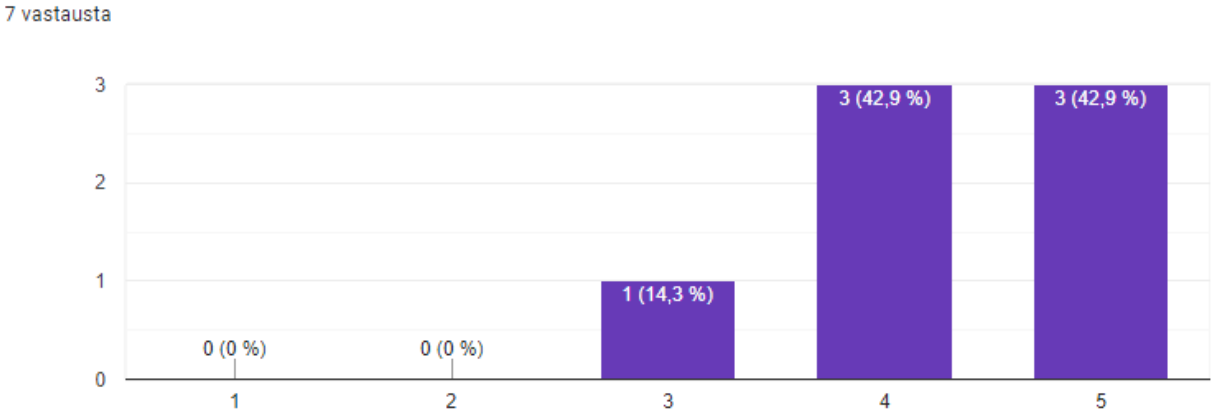
70. Tekoälyavusteinen verkon hallintasovellus (esim. tekoälyavusteinen Network Manager) voisi suunnitella verkon rakenteen vastaamaan haluttua verkon suorituskykyä, kieltää huonot naapuruudet ja poistaa tarpeettomat yhteydet, minkä avulla verkko voidaan rakentaa minimipalveluista täyteen suorituskykyyn. Parempi suorituskyky saadaan silloin, kun ohjaus tehdään verkon hallintatyökalulla (esim. Node Managerista) tai radiosta suoraan ja ohjaus perustuu radioparametrien hyödyntämiseen verkon muodostamisvaiheessa ja myöhemmin koko verkon suorituskyvyn optimoinnissa.



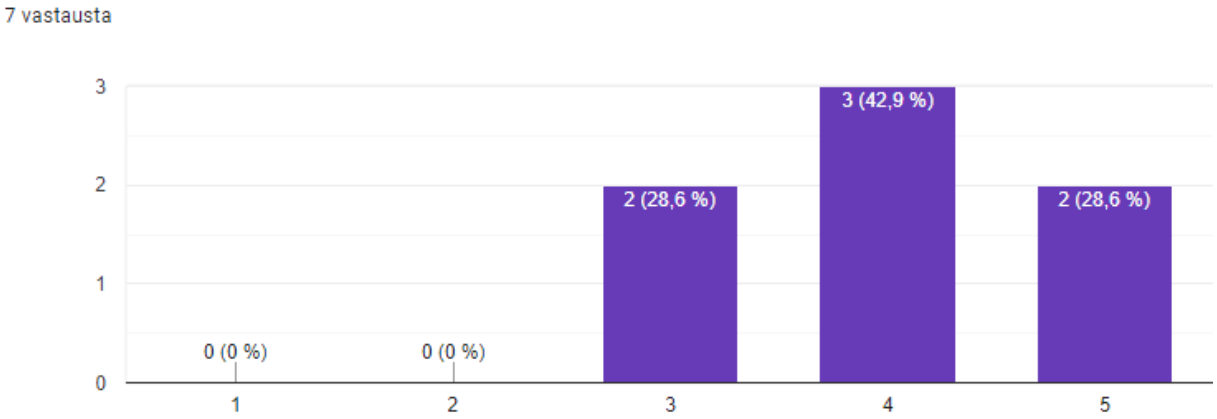
71. Kognitiivisen taktisen verkon ohjauksella tulisi olla rajapinta mahdollisen johtamis- ja tilannekuvajärjestelmän (esim. MATI) kanssa.



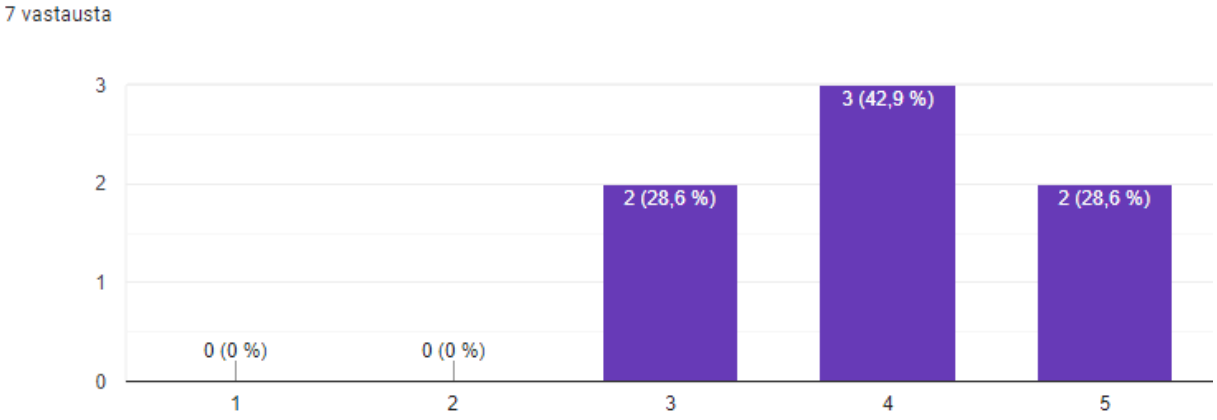
72. Kognitiivisella taktisella verkon tulisi muodostaa havainnoista käyttäjälle helpommin tulkittavissa olevaa dataa visuaalisen käyttöliittymän avulla, jolloin myös käyttäjä pysyy helpommin tilannekuvan tasalla.



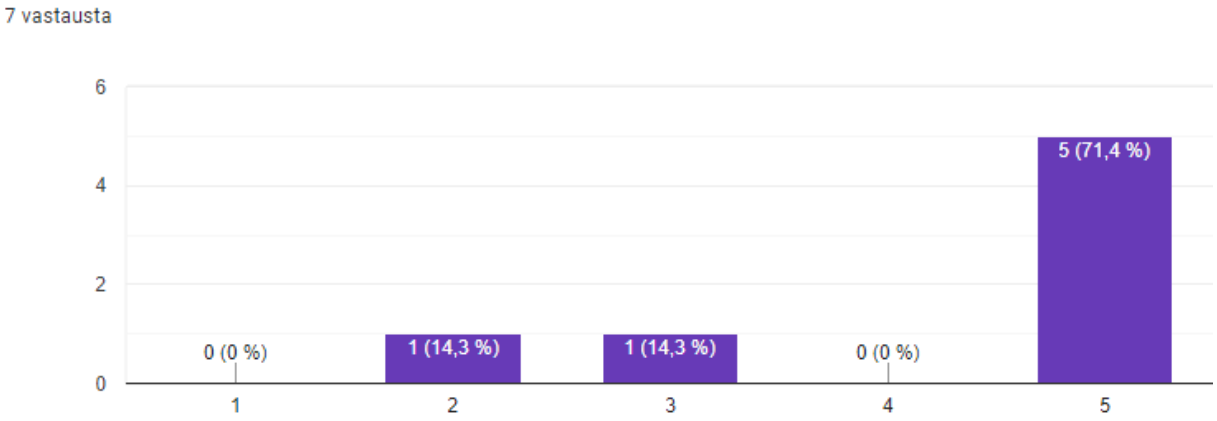
73. Verkon muutoksiin liittyen tulisi olla mahdollisuus käyttäjän hyväksynnälle.



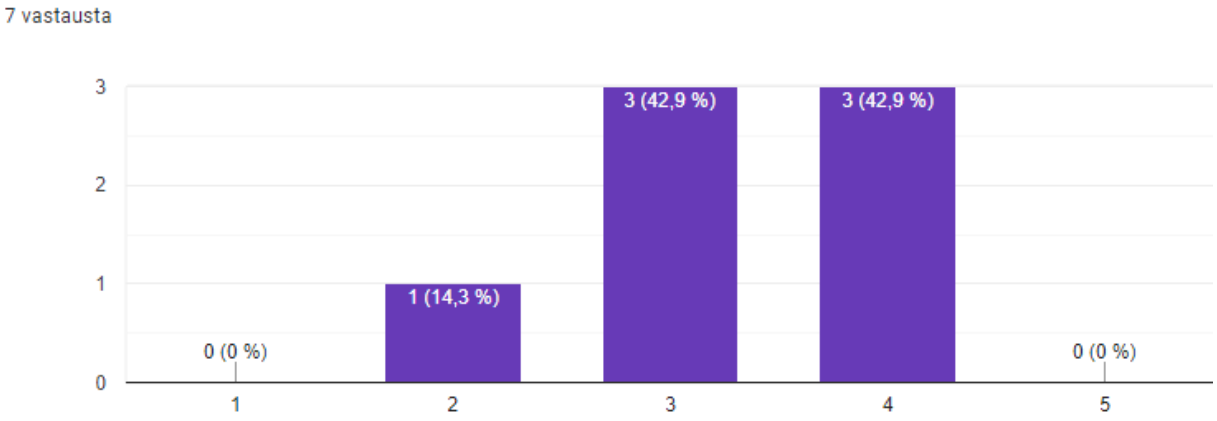
74. Kognitiivisen taktisen verkon tulisi kyetä automaattiseen toimeenpanoon esim. tuottamalla automaattiset asemakäskyt viestiasemille.



75. Kognitiivisen radioverkon tulisi kyetä toimimaan yllättävästi, esimerkiksi vihollisen käyttämän taajuusalueen hyödyntämisellä.



76. Tekoälyn tekemät päätökset tulee tarkastaa järjestelmän ohjaus- ja suunnitteluhenkilöstön toimenpitein.



77. Tekoälylle tulee antaa päätöksentekokyky pieniin parametrien vaihtoon, mutta tekoälyn tulee kyetä myös ennalta esitellä suuremmat optimoinnit ja verkkorakenteen muutokset.